WatchGuard® System Manager User Guide

WatchGuard System Manager



Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

WatchGuard Firebox Software End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This Firebox Software End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD Firebox software product, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product or included on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid. The WATCHGUARD hardware product is subject to a separate agreement and limited hardware warranty included with the WATCHGUARD hardware product packaging and/or in the associated user documentation.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any single WATCHGUARD hardware product at any single location and may install and use the SOFTWARE PRODUCT on multiple workstation computers.

(B) To use the SOFTWARE PRODUCT on more than one WATCHGUARD hardware product at once, you must purchase an additional copy of the SOFTWARE PRODUCT for each additional WATCHGUARD hardware product on which you want to use it. To the extent that you install copies of the SOFTWARE PRODUCT on additional WATCHGUARD hardware products in accordance with the prior sentence without installing the additional copies of the SOFTWARE PRODUCT included with such WATCHGUARD hardware products, you agree that use of any software provided with or included on the additional WATCHGUARD hardware products that does not require installation will be subject to the terms and conditions of this AGREEMENT. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(C) In addition to the copies described in Section 2(A), you may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. United States Government Restricted Rights. The SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6. Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Version: 040226

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2004 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, the WatchGuard logo, Firebox, LiveSecurity, and any other mark listed as a trademark in the "Terms of Use" portion of the WatchGuard Web site that is used herein are either registered trademarks or trademarks of WatchGuard Technologies, Inc. and/or its subsidiaries in the United States and/or other countries. All other trademarks are the property of their respective owners.

Printed in the United States of America.

Part No: 1316-002

U.S. Patent Nos. 6,493,752; 6,597,661; 6,618,755; D473,879. Other Patents Pending.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT®, Windows® 2000 and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All right reserved.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-2003 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-2003 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes' SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2003 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache Software License, Version 1.1

Copyright (c) 2000-2004 The Apache Software Foundation. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

PCRE LICENSE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2003 University of Cambridge

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. In practice, this means that if you use PCRE in software that you distribute to others, commercially or otherwise, you must put a sentence like this:

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

somewhere reasonably visible in your documentation and in any relevant files or online help data or similar. A reference to the ftp site for the source, that is, to:

ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

should also be given in the documentation. However, this condition is not intended to apply to whole chains of software. If package A includes
PCRE, it must acknowledge it, but if package B is software that includes
package A, the condition is not imposed on package B (unless it uses
PCRE independently).

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. If PCRE is embedded in any software that is released under the GNU General Purpose License (GPL), or Lesser General Purpose License (LGPL), then the terms of that license shall supersede any condition above with which it is incompatible.

The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

PLEASE NOTE: Some components of the WatchGuard WFS software incorporate source code covered under the GNU Lesser General Public License (LGPL). To obtain the source code covered under the LGPL, please contact WatchGuard Technical Support at:

877.232.3531 in the United States and Canada
+1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

This product includes software covered by the LGPL.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it

too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of

it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves,

then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during

execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system rather than copying library functions into the executable, and (2) operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to

these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

PLEASE NOTE: Some components of the WatchGuard WFS software incorporate source code covered under the GNU General Public License (GPL). To obtain the source code covered under the GPL, please contact WatchGuard Technical Support at:

877.232.3531 in the United States and Canada
+1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

This product includes software covered by the GPL.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our

decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Software Version: 7.2

Contents

CHAPTER 1 Introduction 1
Welcome to WatchGuard® 1
WatchGuard System Manager Components 2
Minimum Requirements 3
WatchGuard Options 4
Managing and Enabling License Keys 6
About this Guide 7
CHAPTER 2 Service and Support.....9
Benefits of LiveSecurity® Service 9
LiveSecurity® Broadcasts 10
LiveSecurity® Self Help Tools 12
WatchGuard Users Forum 14
WatchGuard Users Group 14
Online Help 15
Product Documentation 17
Assisted Support 17
Training and Certification 19
CHAPTER 3 Getting Started 21
Using an Existing Configuration 22

Gathering Network Information 22
Selecting a Firewall Configuration Mode 25
Setting Up the Management Station 31
Cabling the Firebox 33
Running the QuickSetup Wizard 35
Deploying the Firebox into Your Network 38
What's Next 38
CHAPTER 4 Firebox Basics 41
What is a Firebox? 41
Opening a Configuration File 43
Saving a Configuration File 44
Resetting Firebox Passphrases 47
Setting the Firebox Model 48
Setting the Time Zone 48
Setting a Firebox Friendly Name 48
CHAPTER 5 Using Policy Manager to Configure Your Network 51
Starting a New Configuration File 52
Setting the Firebox Configuration Mode 52
Setting IP Addresses of Firebox Interfaces 52
Setting DHCP or PPPoE Support on the External Interface .54
Configuring Drop-in Mode 56
Defining External IP Aliases 57
Adding Secondary Networks 57
Entering WINS and DNS Server Addresses 58
Configuring Out-of-Band Management 59
Defining a Firebox as a DHCP Server 59
Adding Basic Services to Policy Manager 62
Configuring Routes 62
Specifying Manual or Automatic Settings for Ports 64
CHAPTER 6 Managing and Monitoring the Firebox.....67
About Incoming and Outgoing Traffic 67
Starting System Manager and Connecting to a Firebox 68

Using the Security Traffic Display 69
Basic System Manager Functionality 71
Monitoring Firebox Traffic 75
Performing Basic Tasks with System Manager 77
Viewing Bandwidth Usage 81
Viewing Number of Connections by Service 82
Viewing Details on Firebox Activity 82
HostWatch 91
CHAPTER 7 Configuring Network Address Translation 95
Dynamic NAT 96
Using Simple Dynamic NAT 97
Using Service-Based Dynamic NAT 100
Configuring Service-Based Static NAT 101
Using 1-to-1 NAT 103
Proxies and NAT 105
CHAPTER 8 Configuring Filtered Services 107
Selecting Services for your Security Policy Objectives 108
Adding and Configuring Services 110
Defining Service Properties 117
Service Precedence 122
CHAPTER 9 Configuring Proxied Services 125
Protocol Anomaly Detection 126
Customizing Logging and Notification for Proxies 126
Configuring an SMTP Proxy Service 127
Configuring an FTP Proxy Service 138
Selecting an HTTP Service 140
Configuring the DNS Proxy Service 144
CHAPTER 10 Creating Aliases and Implementing Authentication 149
Using Aliases 150
How User Authentication Works 152
Authentication Server Types 153
Defining Firebox Users and Groups for Authentication 155

Configuring Windows NT Server Authentication 157
Configuring RADIUS Server Authentication 158
Configuring CRYPTOCard Server Authentication 160
Configuring SecurID Authentication 162
CHAPTER 11 Intrusion Detection and Prevention 165
Default Packet Handling 165
Detecting Man-in-the-Middle Attacks 170
Blocking Sites 171
Blocking Ports 174
Blocking Sites Temporarily with Service Settings 179
Integrating Intrusion Detection 179
CHAPTER 12 Setting Up Logging and Notification 183
Developing Logging and Notification Policies 184
Failover Logging 186
WatchGuard Logging Architecture 186
Designating Log Hosts for a Firebox 187
Setting up the WatchGuard Security Event Processor 190
Setting Global Logging and Notification Preferences 194
Customizing Logging and Notification by Service or Option 197
CHAPTER 13 Reviewing and Working with Log Files 203
Log File Names and Locations 203
Viewing Files with LogViewer 204
Displaying and Hiding Fields 206
Working with Log Files 209
CHAPTER 14 Generating Reports of Network Activity 215
Creating and Editing Reports 216
Specifying a Report Time Span 218
Specifying Report Sections 218
Consolidating Report Sections 219
Setting Report Properties 219
Exporting Reports 220
Using Report Filters 222

Scheduling and Running Reports 224
Report Sections and Consolidated Sections 224
CHAPTER 15 Controlling Web Site Access 231
Getting Started with WebBlocker 231
Configuring the WebBlocker Service 233
Managing the WebBlocker Server 238
Installing Multiple WebBlocker Servers 238
Automating WebBlocker Database Downloads 239
CHAPTER 16 Connecting with Out-of-Band Management 241
Connecting a Firebox with OOB Management 241
Enabling the Management Station 242
Configuring the Firebox for OOB 244
Establishing an OOB Connection 245
CHAPTER 17 Introduction to VPN Technology 247
Tunneling Protocols 248
Encryption 249
Authentication 250
Internet Key Exchange (IKE) 250
WatchGuard VPN Solutions 251
CHAPTER 18 Designing a VPN Environment 259
Selecting an Authentication Method 259
Selecting an Encryption and Data Integrity Method 260
IP Addressing 260
NAT and VPNs 261
Access Control 261
Network Topology 262
Tunneling Methods 264
Determining Which WatchGuard VPN Solution to Use 265
VPN Scenarios 267
CHAPTER 19 Activating the Certificate Authority on the Firebox 271
Public Key Cryptography and Digital Certificates 272
PKI in a WatchGuard VPN 272

Defining a Firebox as a DVCP Server and CA 275
Managing the Certificate Authority 278
CHAPTER 20 Configuring RUVPN with PPTP 281
Configuration Checklist 281
Configuring WINS and DNS Servers 283
Adding New Users to Authentication Groups 284
Configuring Services to Allow Incoming RUVPN Traffic 285
Activating RUVPN with PPTP 287
Enabling Extended Authentication 288
Entering IP Addresses for RUVPN Sessions 288
Configuring Debugging Options 289
Preparing the Client Computers 289
Windows NT Platform Preparation 290
Windows 2000 Platform Preparation 293
Windows XP Platform Preparation 293
Starting RUVPN with PPTP 294
Running RUVPN and Accessing the Internet 294
Making Outbound PPTP Connections From Behind a Firebox 295
Making Outbound IPSec Connections From Behind a Firebox 295
CHAPTER 21 Configuring BOVPN with Basic DVCP 297
Configuration Checklist 298
Creating a Tunnel to a Device 298
Configuring Logging for a DVCP Server 301
CHAPTER 22 Configuring BOVPN with Manual IPSec 303
Configuration Checklist 304
Configuring a Gateway 304
Creating a Tunnel with Manual Security 308
Creating a Tunnel with Dynamic Key Negotiation 311
Creating a Routing Policy 312
Enabling the BOVPN Upgrade 317

CHAPTER 23 Configuring IPSec Tunnels with VPN Manager 319
Defining a Firebox as a DVCP Server and CA 320
Launching VPN Manager 320
Adding Devices to VPN Manager (Dynamic Devices Only) 321
Defining a Firebox as a DVCP Client (Dynamic Fireboxes Only) 323
Adding Policy Templates (Required for Dynamic Devices) 324
Adding Security Templates 325
Creating Tunnels Between Devices 326
Enabling a SOHO Single-Host Tunnel 328
Editing a Tunnel 330
Removing Tunnels and Devices from VPN Manager 330
Allowing Remote Access to the DVCP Server 331
CHAPTER 24 Monitoring VPN Devices and Tunnels 333
Monitoring VPNs from System Manager 333
Monitoring VPNs through VPN Manager 336
CHAPTER 25 Managing the SOHO 6 with VPN Manager 341
Importing Certificates 341
Accessing the SOHO 6 344
Removing Certificates 347
CHAPTER 26 Troubleshooting Firebox Connectivity 349
Method 1: Ethernet Dongle Method 349
Method 2: The Flash Disk Management Utility 352
Method 3: Using the Reset Button 354

Index 357

CHAPTER 1

Introduction

Welcome to WatchGuard®

In the past, a connected enterprise needed a complex set of tools, systems, and personnel for access control, authentication, virtual private networking, network management, and security analysis. These costly systems were difficult to integrate and not easy to update. Today, WatchGuard System Manager delivers a complete network security solution to meet these modern security challenges:

- Keeping network defenses current
- Protecting every office connected to the Internet
- Encrypting communications to remote offices and traveling users
- Managing the security system from a single site

WatchGuard System Manager is a reliable, flexible, scalable, and inexpensive network security solution. Its setup and maintenance costs are small, and it supports a rich feature set. When properly configured and administered, WatchGuard System Manager reliably defends any network against external threats.

WatchGuard System Manager Components

WatchGuard System Manager has all of the components needed to conduct electronic business safely. It is made up of the following:

- Firebox—an integrated security appliance
- Firebox System Manager—a suite of management and monitoring tools
- A collection of advanced security applications
- LiveSecurity® Service—a security-related broadcast service

WatchGuard Firebox

The Firebox family of products is specially designed and optimized. These machines are small, efficient, and reliable. The Firebox X has an indicator display and physical interfaces on its front panel. The Firebox III has an indicator display panel in front and physical interfaces in back.

Firebox System Manager

Firebox System Manager is a toolkit of applications run from a single location, enabling you to configure, manage, and monitor your network security policy. In addition to management and monitoring tools, System Manager includes:

Policy Manager
Allows you to design, configure, and manage a network security policy.

LogViewer
Displays a static view of the log data, which you can filter by type, search for keywords and fields, and print and save to a separate file.

HostWatch
Displays active connections occurring on a Firebox in real time or represents the connections listed in a log file.

Historical Reports
Creates HTML reports that display session types, most active hosts, most used services, URLs, and other data useful in monitoring and troubleshooting your network.

WatchGuard security applications

In addition to basic security policy configuration, WatchGuard System Manager includes a suite of advanced software features. These include:

- User authentication
- Network address translation
- Remote user virtual private networking
- Branch office virtual private networking
- Selective Web site blocking

WatchGuard LiveSecurity® Service

The innovative LiveSecurity Service makes it easy to maintain the security of an organization's network. WatchGuard's team of security experts publish alerts and software updates, which are broadcast to your email client.

Minimum Requirements

This section describes the minimum hardware and software requirements necessary to successfully install, run, and administer WatchGuard System Manager.

Software requirements

WatchGuard System Manager software can run on Microsoft Windows NT 4.0, Windows 2000, or Windows XP as specified below:

Windows NT requirements

- Microsoft Windows NT 4.0
- Microsoft Service Pack 4, Service Pack 5, or Service Pack 6a for Windows NT 4.0

Windows 2000 requirements

- Microsoft Windows 2000 Professional or Windows 2000 Server

Windows XP requirements

- Microsoft Windows XP

Web browser requirements

You must have Microsoft Internet Explorer 4.0 or later to run the installation from the CD. The following HTML-based browsers are recommended to view WatchGuard Online Help:

- Netscape Communicator 4.7 or later
- Microsoft Internet Explorer 5.01 or later

Hardware requirements

Minimum and recommended hardware requirements are listed on the following table.

Hardware feature	Minimum	Recommended
Memory	128 MB	256 MB
Processor	700 MHz	1.4 GHz
Hard disk space	100 MB	1 GB

WatchGuard Options

WatchGuard System Manager is enhanced by optional features designed to accommodate the needs of different customer environments and security requirements.

The following options are currently available for WatchGuard System Manager.

Firebox X 3-Port Upgrade

Purchase this option to activate three additional network ports on your Firebox X. You can use the additional ports to create DMZs for public servers, or you can protect additional internal segments of your network with your Firebox. Enhancing your Firebox X with this upgrade adds new functionality using the same configuration tools and methods as described for your optional port.

Firebox X Model Upgrade

If you have a Firebox X500, you can purchase an upgrade to make your Firebox function as a Firebox 700, 1000, or 2500.

VPN Manager

WatchGuard VPN Manager is a centralized module for creating and managing the network security of an organization that uses

the Internet to conduct business. It turns the complex task of setting up multi-site virtual private networks (VPNs) into a simple three-step process. VPN Manager sets a new standard for Internet security by automating the setup, management, and monitoring of multi-site IPSec VPN tunnels between an organization's headquarters, branch offices, telecommuters, and remote users.

High Availability

WatchGuard High Availability software lets you install a second, standby Firebox on your network. If your primary Firebox fails, the second Firebox automatically takes over to give your customers, business partners, and employees virtually uninterrupted access to your protected network.

Mobile User VPN

Mobile User VPN is the WatchGuard IPSec implementation of remote user virtual private networking. Mobile User VPN connects an employee on the road or working from home to networks behind a Firebox using a standard Internet connection, without compromising security. WatchGuard Mobile User VPN software easily integrates into WatchGuard System Manager, allowing your mobile users to securely connect to your network. VPN traffic is encrypted using DES or 3DES-CBC, and authenticated through MD5 or SHA-1.

SpamScreen

SpamScreen helps to control "spam"—email sent to you or your end users without permission. Spam consumes valuable bandwidth on your Internet connection and on the hard disk space and CPU time of your mail server. If allowed to enter your network unchecked, spam consumes workers' time to read and remove. WatchGuard SpamScreen identifies spam as it comes through the Firebox. You can choose to either block the spam at the Firebox or tag it for easy identification and sorting.

BOVPN Upgrade

The factory default Firebox III 500 or Firebox X500 does not support branch office VPN. However, you can purchase the BOVPN Upgrade option to enable BOVPN support on a Firebox 500.

BOVPN is supported on the Firebox X700, Firebox X1000, and Firebox X2500, but you must register the device with LiveSecurity Service to obtain the BOVPN feature key. BOVPN is available by default on other models.

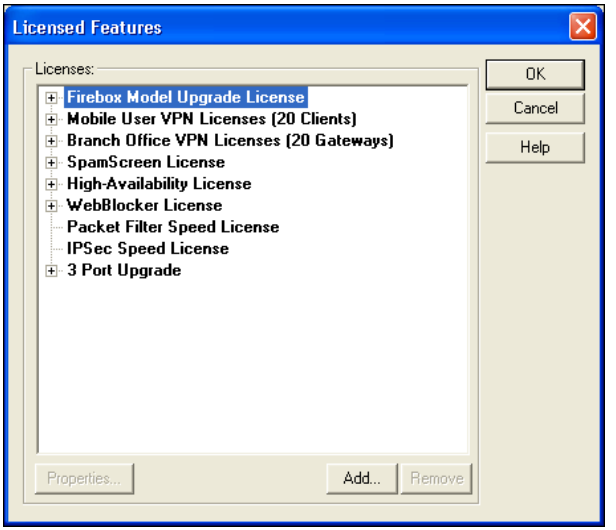
Obtaining WatchGuard Options

WatchGuard options are available from your local reseller. For more information about purchasing WatchGuard products, go to:
http://www.watchguard.com/sales/

Managing and Enabling License Keys

To enable any WatchGuard option, you must add it to the **Licensed Features** dialog box. You can also use this dialog box to view or delete license keys.

1 From Policy Manager, select **Setup** ⇒ **Licensed Features**.
The Licensed Features dialog box appears.



2 Click **Add**.

3 In the **Add/Import License Keys** dialog box, either type your license key or click **Browse** and find it on your network. Click **OK**.
The new license now appears on the Licensed Features dialog box.

4 To view a license key, select the license key and click **Properties**.
To delete a license key, select the license key and click **Remove**.

About this Guide

The purpose of this guide is to help users of WatchGuard System Manager set up and configure a basic network security system and maintain, administer, and enhance the configuration of their network security.

The audience for this guide represents a wide range of experience and expertise in network management and security. The end user of WatchGuard System Manager is generally a network administrator for a company that can range from a small branch office to a large enterprise with multiple offices around the world.

References to FAQs, on the online support pages, are included throughout this guide. To access the FAQs, you must have a current subscription to the LiveSecurity Service.

The following conventions are used in this guide:

- The term “Firebox” refers to either the Firebox III or the Firebox X unless specifically stated. Illustrations of Fireboxes are interchangeable unless specifically stated.
- Within procedures, visual elements of the user interface, such as buttons, menu items, dialog boxes, fields, and tabs, appear in boldface.
- Menu items separated by arrows (⇒) are selected in sequence from subsequent menus. For example, **File** ⇒ **Open** ⇒ **Configuration File** means to select **Open** from the **File** menu, and then **Configuration File** from the **Open** menu.
- Code, messages, and file names appear in monospace font; for example: `.wgl` and `.idx` files

- In command syntax, variables appear in italics; for example: fbidsmate *import_passphrase*
- Optional command parameters appear in square brackets.

CHAPTER 2

Service and Support

No Internet security solution is complete without systematic updates and security intelligence. From the latest hacker techniques to the most recently discovered operating system bug, the daily barrage of new threats poses a perpetual challenge to any network security solution. LiveSecurity® Service keeps your security system up-to-date by providing solutions directly to you.

In addition, the WatchGuard Technical Support team and Training department offer a wide variety of methods to answer your questions and assist you with improving the security of your network.

Benefits of LiveSecurity® Service

As the frequency of new attacks and security advisories continues to surge, the task of ensuring that your network is secure becomes an even greater challenge. The WatchGuard Rapid Response Team, a dedicated group of network security experts, helps absorb this burden by monitoring the Internet security landscape for you in order to identify new threats as they emerge.

Threat alerts and expert advice

After a new threat is identified, you'll receive a LiveSecurity broadcast by way of an email message from our Rapid Response Team that alerts you to the threat. Each alert includes a complete description of the nature and severity of the threat, the risks it poses, and what steps you should take to make sure your network remains continuously protected.

Easy software updates

Your WatchGuard LiveSecurity Service subscription saves you time by providing the latest software to keep WatchGuard System Manager up-to-date. You receive installation wizards and release notes with each software update for easy installation. These ongoing updates ensure that WatchGuard System Manager remains state-of-the-art, without you having to take time to track new releases.

Access to technical support and training

When you have questions about your WatchGuard system, you can quickly find answers using our extensive online support resources, or by talking directly to one of our support representatives. In addition, you can access WatchGuard courseware online to learn about WatchGuard system features.

LiveSecurity® Broadcasts

The WatchGuard LiveSecurity Rapid Response Team periodically sends broadcasts and software information directly to your desktop by way of email. Broadcasts are divided into channels to help you immediately recognize and process incoming information.

Information Alert

Information Alerts provide timely analysis of breaking news and current issues in Internet security combined with the proper system configuration recommendations necessary to protect your network.

Threat Response
After a newly discovered threat is identified, the Rapid Response Team transmits an update specifically addressing this threat to make sure your network is protected.

Software Update
You receive functional software enhancements on an ongoing basis that cover your entire WatchGuard System Manager.

Editorial
Leading security experts join the WatchGuard Rapid Response Team in contributing useful editorials to provide a source of continuing education on this rapidly changing subject.

Foundations
Articles specifically written for novice security administrators, non-technical co-workers, and executives.

Loopback
A monthly index of LiveSecurity Service broadcasts.

Support Flash
These technical tutorials provide tips for managing WatchGuard System Manager. Support Flashes supplement other resources such as Online Help, FAQs, and Known Issues pages on the Technical Support Web site.

Virus Alert
In cooperation with McAfee, WatchGuard issues weekly broadcasts that provide the latest information on new computer viruses.

New from WatchGuard
To keep you abreast of new features, product upgrades, and upcoming programs, WatchGuard first announces their availability to our existing customers.

Activating the LiveSecurity® Service

The LiveSecurity Service can be activated through the setup wizard on the CD-ROM or through the activation section of the WatchGuard LiveSecurity Web pages. The setup wizard is

detailed thoroughly in the QuickStart Guide and in the "Getting Started" chapter of this book.

To activate the LiveSecurity Service through the Web:

1 Be sure that you have the LiveSecurity license key and the Firebox serial number handy. You will need these during the activation process.
   - The Firebox serial number is displayed in two locations: a small silver sticker on the outside of the shipping box, and a sticker on the back of the Firebox just below the UPC bar code
   - The license key number is located on the WatchGuard LiveSecurity Agreement License Key Certificate. Enter the number in the exact form shown on the key, including the hyphens.

2 Using your Web browser, go to: http://www.watchguard.com/account/register.asp
The Account page appears.

NOTE

You must have JavaScript enabled on your browser to be able to activate the LiveSecurity Service.

3 Complete the LiveSecurity Activation form. Move through the fields on the form using either the TAB key or the mouse.
All of the fields are required for successful registration. The profile information helps WatchGuard target information and updates to your needs.

4 Verify that your email address is correct. You will receive your activation confirmation mail and all of your LiveSecurity broadcasts at this address.

5 Click **Register**.

LiveSecurity® Self Help Tools

Online support services help you get the most out of your WatchGuard products.

NOTE

You must register for LiveSecurity Service before you can access the online support services.

Advanced FAQs (frequently asked questions)
Detailed information about configuration options and interoperability.

Basic FAQs
General questions about WatchGuard System Manager.

Known Issues
Confirmed issues and fixes for current software.

Interactve Support Forum
A moderated Web board about WatchGuard products.

Online Training
Information on product training, certification, and a broad spectrum of publications about network security and WatchGuard products. These courses are designed to guide users through all components of WatchGuard products. These courses are modular in design, allowing you to use them in a manner most suitable to your learning objectives. For more information, go to: www.watchguard.com/training/courses_online.asp

Learn About
A listing of all resources available for specific products and features.

Online Help
Current Help system for WatchGuard products.

Product Documentation
A listing of current product documentation from which you can open `.pdf` files.

General SOHO 6 Resources
Access to the resources you need and updated information to help you install and use the SOHO 6.

To access the online support services:

1 From your Web browser, go to http://www.watchguard.com/ and click **Support**.

2 Log in to LiveSecurity Service.

WatchGuard Users Forum

The WatchGuard users forum is an online group in which the users of WatchGuard System Manager exchange ideas, questions, and tips regarding all aspects of the product, including configuration, compatibility, and networking. This forum is categorized and searchable, and is moderated, during regular business hours, by WatchGuard engineers and Technical Support personnel. However, this forum should not be used for reporting support issues to WatchGuard Technical Support. Instead, contact WatchGuard Technical Support directly by way of the Web interface or telephone.

Joining the WatchGuard users forum

To join the WatchGuard users forum:

1 Go to www.watchguard.com. Click **Support**. Log into the LiveSecurity Service.

2 Under **Self-Help Tools**, click **Interactive Support Forum**.

3 Click **Create a User Forum account**.

4 Enter the required information in the form. Click **Create**.
The username and password should be of your own choosing. They should not be the same as that of your LiveSecurity Service.

WatchGuard Users Group

The WatchGuard users group is an online group in which the users of WatchGuard products can communicate information. Because this group is not monitored by WatchGuard, it should not be used for reporting support issues to WatchGuard Technical Support. Instead, contact WatchGuard Technical Support directly via the Web interface or telephone. For information on how to subscribe, unsubscribe, or post a message to all WG-user members, go to:

http://lists.watchguard.com/mailman/listinfo/wg-users

Online Help

WatchGuard Online Help is a Web-based system with cross-platform functionality that enables you to install a copy on virtually any computer. A static version of the Online Help system is installed automatically with the WatchGuard System Manager software in a subdirectory of the installation directory called `Help`. In addition, a "live," continually updated version of Online Help is available at:

http://www.watchguard.com/help

You may need to log into the LiveSecurity Service to access the Online Help system.

Starting WatchGuard Online Help

WatchGuard Online Help can be started either from the WatchGuard management station or directly from a browser.

- In the management station software (any WatchGuard System Manager window or dialog box), press F1.
- On any platform, browse to the directory containing WatchGuard Online Help. Open LSSHelp.html. The default help directory is C:\Program Files\WatchGuard\Help.

Searching for topics

You can search for topics in WatchGuard Online Help three ways:

Contents

The **Contents** tab displays a list of topics within the Help system. Double-click a book to expand a category. Click a page title to view topic contents.

Index

The index provides a list of keywords found within Help. Begin typing the keyword, and the index list will automatically scroll to entries beginning with those letters. Click a page title to view topic contents.

Search

The Search feature offers a full-text search of the entire Help system. Enter a keyword. Press ENTER to display a list of

topics containing the word. The Search feature does not support Boolean searches.

Copying the Help system to additional platforms

WatchGuard Online Help can be copied from the management station to additional workstations and platforms. When doing so, copy the entire Help directory from the WatchGuard installation directory on the management station. It is important to include all subdirectories exactly as they appear in the original installation.

Online Help system requirements

Web browser

- Internet Explorer 4.0 or higher
- Netscape Navigator 4.7 or higher

Operating system

- Windows NT 4.0, Windows 2000, or Windows XP
- Sun Solaris
- Linux

Context-sensitive Help

In addition to the regular online Help system, context-sensitive or What's This? Help is also available. What's This? Help provides a definition and useful information on fields and buttons in the dialog boxes. To access What's This? Help:

1. Right-click any field or button.
2. Click **What's This?** when it appears.
   A box appears with the field name on the top and information about the field beneath it.
3. To print or save the Help box as a separate file, right-click the **Help** field.
   A menu offering Copy or Print appears.
4. Select the menu item you want.
5. When you are done, click anywhere outside the box to dismiss it.

You can also look up the meaning of fields and buttons using the "Field Definitions" chapter in the *Reference Guide*.

Product Documentation

WatchGuard products are fully documented on our Web site at: http://www.watchguard.com/help/documentation/

Assisted Support

WatchGuard offers a variety of technical support services for your WatchGuard products. Several support programs, described throughout this section, are available through WatchGuard Technical Support. For a summary of the current technical support services offered by WatchGuard Technical Support, please refer to the WatchGuard Web site at: http://www.watchguard.com/support

NOTE

You must register for LiveSecurity Service before you can receive technical support.

LiveSecurity® Program

WatchGuard LiveSecurity Technical Support is included with every new Firebox. This support program is designed to assist you in maintaining your enterprise security system involving our Firebox, SOHO, and VPN products.

Hours

WatchGuard LiveSecurity Technical Support business hours are 6:00 AM to 6:00 PM in your local time zone, Monday through Friday.

Phone Contact

877.232.3531 in U.S. and Canada
+1.206.613.0456 all other countries

Web Contact

http://www.watchguard.com/support

Response Time

Four (4) business hours maximum target

Type of Service

Technical assistance for specific issues concerning the installation and ongoing maintenance of Firebox and SOHO enterprise systems

Single Incident Priority Response Upgrade (SIPRU) and Single Incident After-hours Upgrade (SIAU) are available. For more information, please refer to the WatchGuard Web site at: http://www.watchguard.com/support

LiveSecurity® Gold Program

This premium program is designed to meet the aggressive support needs of companies that are heavily dependent upon the Internet for Web-based commerce or VPN tunnels.

WatchGuard Gold LiveSecurity Technical Support offers support coverage 24 hours a day, seven days a week. Our Priority Support Team staffs our support center continuously from 7 PM Sunday to 7 PM Friday Pacific Time, and can help you with any technical issues you might have during these hours.

We target a one-hour maximum response time for all new incoming cases. If a technician is not immediately available to help you, a support administrator will log your call in our case response system and issue a support incident number.

Firebox Installation Services

WatchGuard Remote Firebox Installation Services are designed to provide you with comprehensive assistance for basic Firebox installation. You can schedule a dedicated two-hour time slot with one of our WatchGuard technicians to help you review your network and security policy, install the LiveSecurity software and Firebox hardware, and build a configuration in accordance with your company security policy. VPN setup is not included as part of this service.

VPN Installation Services

WatchGuard Remote VPN Installation Services are designed to provide you with comprehensive assistance for basic VPN installation. You can schedule a dedicated two-hour time slot with one of our WatchGuard technicians to review your VPN policy, help you configure your VPN tunnels, and test your VPN config-

uration. This service assumes you have already properly installed and configured your Fireboxes.

Training and Certification

WatchGuard offers product training, certification, and a broad spectrum of publications to customers and partners who want to learn more about network security and WatchGuard products. Designed to quickly bring you up to speed on network security issues and our award-winning product line, you will learn exactly what you need to do to protect valuable information assets and make the most of your WatchGuard products. No matter where you are located or which products you own, we have a training solution for you.

WatchGuard classroom training is available worldwide through an extensive network of WatchGuard Certified Training Partners (WCTPs). WCTPs strengthen our relationships with our partners and customers by providing top-notch instructor-led training in a local setting.

WatchGuard offers product and sales certification, focusing on acknowledging the skills necessary to configure, deploy, and manage enterprise security solutions.

CHAPTER 3

Getting Started

WatchGuard System Manager acts as a barrier between your networks and the public Internet, protecting them from security threats. This chapter explains how to install WatchGuard System Manager into your network. You must complete the following steps in the installation process:

- Gathering network information
- Selecting a firewall configuration model
- Setting up the management station
- Cabling the Firebox
- Running the QuickSetup Wizard
- Deploying the Firebox into your network

For a quick summary of this information, see the WatchGuard Firebox *QuickStart Guide* included with your Firebox.

NOTE

This chapter assumes your Firebox has the default three-port configuration. If you have purchased the Firebox X 3-Port Upgrade, use the same configuration tools and methods as described for your optional port.

Before installing WatchGuard System Manager, check the package contents to make sure you have the following items:

- WatchGuard Firebox security appliance
- QuickStart Guide
- User documentation
- WatchGuard System Manager CD-ROM
- A serial cable (blue)
- Three crossover ethernet cables (red)
- Three straight ethernet cables (green)
- Power cable
- LiveSecurity® Service license key

Using an Existing Configuration

This chapter is intended for new WatchGuard System Manager installations only. If you have an existing configuration, open it with Policy Manager. You will be prompted to convert to the new version.

If your configuration is more than one version back, you may experience conversion problems. If this happens, consider building a new configuration.

Gathering Network Information

We encourage you to fill in the following tables in preparation for completing the rest of the installation process.

License Keys

Collect your license key certificates. WatchGuard System Manager comes with a LiveSecurity Service key that activates your 90 day subscription to the LiveSecurity Service.

For more information on this service, see Chapter 2, “Service and Support.” High Availability and SpamScreen are optional products, and you receive those license keys upon purchase. For more information on optional products, see Chapter 1, “Introduction.”

Network addresses

One good way to set up your network is to create two worksheets: the first worksheet represents your network now—before

deploying the Firebox—and the second represents your network after the Firebox is deployed. Fill in the IP addresses in the worksheets below.

Network Before Firebox

_____ . _____ . _____ . _____ /_____
Public Network/subnet

_____ . _____ . _____ . _____
Internet Router

_____ . _____ . _____ . _____ /_____
Local LAN/subnet

_____ . _____ . _____ . _____ /_____
Secondary Network (if applicable)

_____ . _____ . _____ . _____
Public Server

_____ . _____ . _____ . _____
Internet router for remote network (if applicable)

Network with Firebox

_____ . _____ . _____ . _____
Default Gateway of Firebox (Internet Router)

_____ . _____ . _____ . _____ /_____
External Interface (where Firebox connects to Internet router)

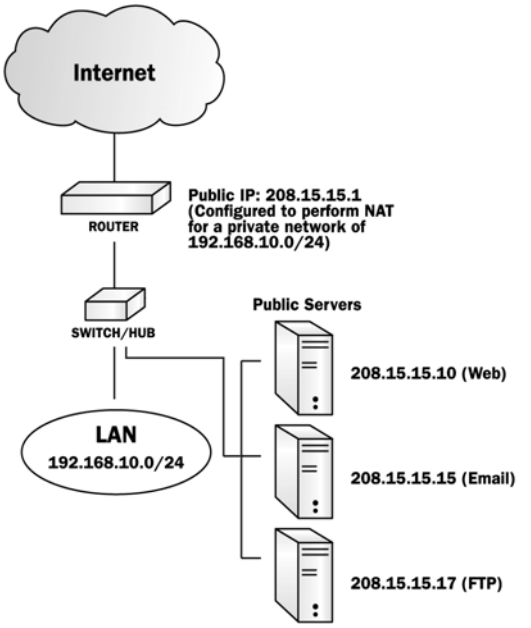
_____ . _____ . _____ . _____
Trusted Interface

_____ . _____ . _____ . _____ /_____
Optional Interface (if applicable)

_____ . _____ . _____ . _____ /_____
Secondary network (if applicable)

An example of a network before the Firebox is installed appears in the following figure. In this example, the Internet router performs network address translation (NAT) for the internal net-

work. The router has a public IP address of 208.15.15.1, and the private network has an address of 192.168.10.0/24. This network also has three public servers with the addresses 208.15.15.10, 208.15.15.15, and 208.15.15.17.

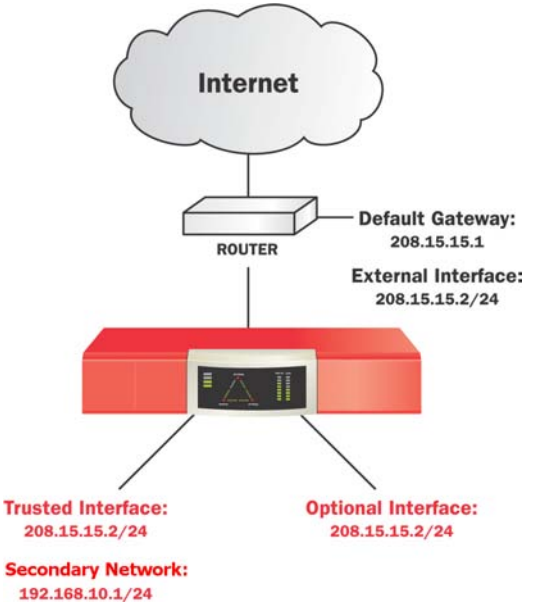


The following figure shows the same example network with a Firebox deployed. The IP address of the Internet router in the previous figure becomes the IP address of the Firebox's default gateway. This network uses drop-in configuration because the public servers will maintain their own IP addresses. Drop-in configuration simplifies the setup of these devices. For more information on this type of configuration, see "Drop-in configuration" on page 27.

By configuring the optional interface on the example network, the public servers can be connected directly to the Firebox (because they are on the same subnet as the Firebox).

In the example, the secondary network represents the local LAN. Because the trusted interface is being configured with the public IP address, a secondary network is added with an unassigned

private IP address from the local LAN: 192.168.10.1/24. This IP address then becomes the default gateway for devices on the local LAN.



Selecting a Firewall Configuration Mode

Before installing WatchGuard System Manager, you must decide how to incorporate the Firebox into your network. This decision determines how you will set up the Firebox interfaces.

External interface
Connects to the external network (typically the Internet) that presents the security threat.

Trusted interface
Connects to the private LAN or internal network that you want protected.

Optional interface
Connects to the DMZ (Demilitarized Zone) or mixed trust area of your network. Computers on the optional interface

contain content you do not mind sharing with the rest of the world. Common applications housed on this interface are Web, email, and FTP servers.

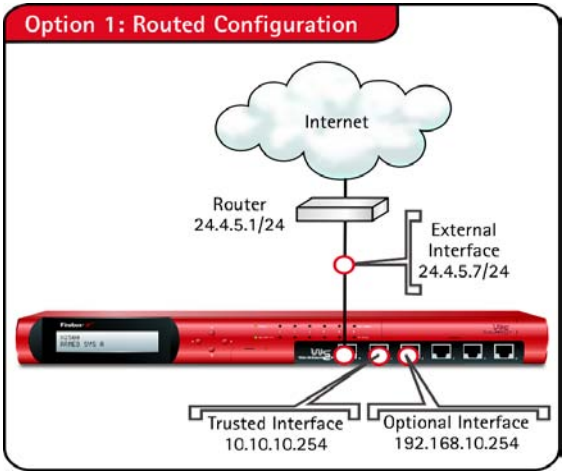
eth3, eth4, eth5

If you purchased the Firebox X 3-port upgrade, you will have three additional ports to connect to the mixed trust area of your network.

To decide how to incorporate the Firebox into your network, select the configuration mode that most closely reflects your existing network. You must select one of two possible modes: routed or drop-in configuration.

Routed configuration

In a routed configuration, the Firebox is put in place with separate logical networks and separate network addresses on its interfaces. Routed configuration is used primarily when the number of public IP addresses is limited or when you have dynamic IP addressing on the external interface. For more information on dynamic IP addressing on the external interface, see “Dynamic IP support on the external interface” on page 30. Public servers behind the Firebox use private addresses, and traffic is routed using network address translation (NAT).



Note: IP addresses in this diagram are examples only. The actual IP addresses must be public addresses.

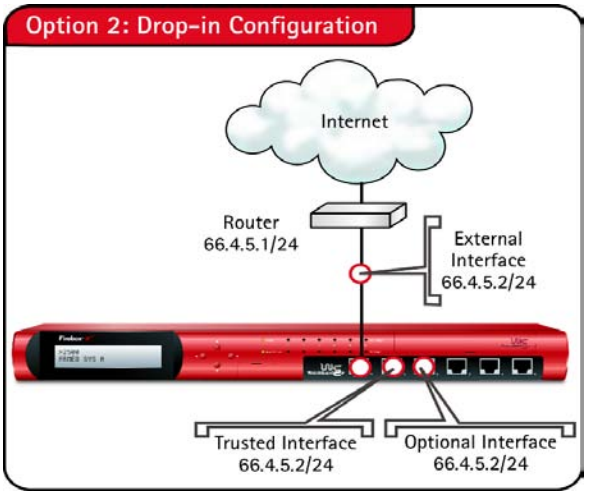
Characteristics of a routed configuration:

- All interfaces of the Firebox must be on different networks. The minimum setup involves the external and trusted interfaces. These are typically private networks.
- The trusted and optional interfaces must be on separate networks and all machines behind the trusted and optional interfaces must be configured with an IP address from that network.

The benefit of a routed configuration is that the networks are well defined and easier to manage, especially regarding VPNs.

Drop-in configuration

In a drop-in configuration, the Firebox is put in place with the same network address on all Firebox interfaces. All three Firebox interfaces must be configured. Because this configuration mode distributes the network's logical address space across the Firebox interfaces, you can "drop" the Firebox between the router and the LAN without reconfiguring any local machines. Public servers behind the Firebox use public addresses, and traffic is routed through the Firebox with no network address translation.



Note: IP addresses in this diagram are examples only. The actual IP addresses must be public addresses.

Characteristics of a drop-in configuration:

- A single network that is not subdivided into smaller networks or subnetted.
- The Firebox performs proxy ARP, a technique in which one host answers Address Resolution Protocol requests for machines behind that Firebox that cannot hear the broadcasts. The trusted interface ARP address replaces the router's ARP address.
- The Firebox can be placed in a network without changing default gateways on the trusted hosts. This is because the Firebox answers for the router, even though the router cannot hear the trusted host's ARP requests. It is common practice to use the Firebox, after it is in place, as a gateway instead of the router.
- All trusted computers must have their ARP caches flushed.
- The majority of a LAN resides on the trusted interface by creating a secondary network for the LAN.

The benefit of a drop-in configuration is that you don't have to reconfigure machines already on a public network with private IP addresses. The drawback is that it is generally harder to manage and is more prone to network problems.

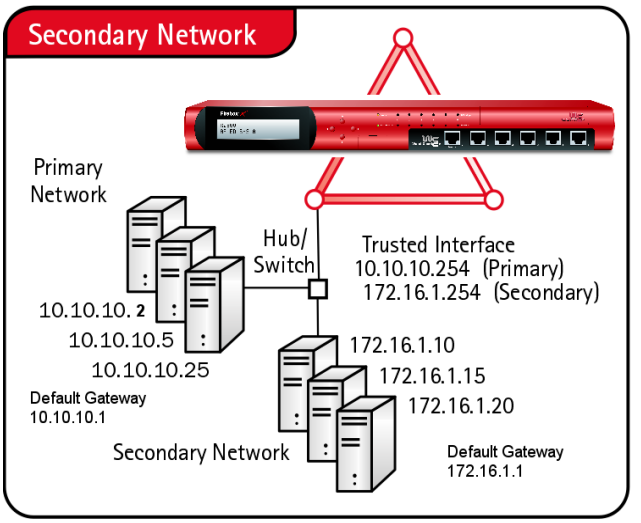
Choosing a Firebox configuration

The decision between routed and drop-in mode is based on your current network. Many networks are best served by routed mode. However, drop-in mode is recommended if you have a large number of public IP addresses, you have a static external IP address, or you are not willing or able to reconfigure machines on your LAN. The following table summarizes the criteria for choosing a Firebox configuration. (For illustrative purposes, it is assumed that the drop-in IP address is a public address.)

	Routed Configuration	Drop-in Configuration
Criterion 1	All interfaces of the Firebox are on different networks. Minimum configured are external and trusted.	All interfaces of the Firebox are on the same network and have the same IP address (Proxy ARP).
Criterion 2	Trusted and optional interfaces must be on separate networks and must use IP addresses drawn from those networks. Both interfaces must be configured with an IP address on the same network, respectively.	Machines on the trusted or optional interfaces can be configured with a public IP address.
Criterion 3	Use static NAT to map any public addresses to private addresses behind the trusted or optional interfaces.	Because machines that are publicly accessible have public IP addresses, no static NAT is necessary.

Adding secondary networks to your configuration

Whether you have chosen routed or drop-in, your configuration may require that you add secondary networks to any of the three Firebox interfaces. A secondary network is a separate network connected to a Firebox interface by a switch or hub.



When you add a secondary network, you map an IP address from the secondary network to the IP address of the Firebox interface. This is known as creating (or adding) an IP alias to the network interface. This IP alias becomes the default gateway for all the machines on the secondary network. The presence of a secondary network also tells the Firebox that another network resides on the Firebox interface wire.

You add secondary networks in the following two ways:

- The QuickSetup Wizard, which is part of the installation process, asks you to select the checkbox if you have "an additional private network behind the Firebox" when you are entering the IP addresses for the Firebox interfaces. The additional private network you specify becomes the secondary network on the trusted interface. For more information on the QuickSetup Wizard, see "Running the QuickSetup Wizard" on page 35.
- After you have finished with the installation, you can add secondary networks to any interface using Policy Manager, as described in "Adding Secondary Networks" on page 57.

Dynamic IP support on the external interface

If you are supporting dynamic IP addressing, you must choose routed configuration.

If you choose the Dynamic Host Configuration Protocol (DHCP) option, the Firebox will request its IP address, gateway, and netmask from a DHCP server managed by your Internet Service Provider (ISP). This server can also provide WINS and DNS server information for your Firebox. If it does not, you must add it manually to your configuration, as described in "Entering WINS and DNS Server Addresses" on page 58. You can also change the WINS and DNS values provided by your ISP, if necessary.

Point-to-Point Protocol over Ethernet (PPPoE) is also supported. As with DHCP, the Firebox initiates a PPPoE protocol connection to your ISP's PPPoE server, which automatically configures your IP address, gateway, and netmask. However, PPPoE does not propagate DNS and WINS server information as DHCP does.

If you are using PPPoE on the external interface, you will need the PPP user name and password when you set up your net-

work. Both username and password each have a 256-byte capacity.

When the Firebox is configured such that it obtains its IP addresses dynamically, the following functionality (which requires a static IP address) is not supported:

- High Availability (not supported on Firebox 500)
- Drop-in mode
- 1-to-1 NAT
- Enabling the Firebox as a DVCP server
- BOVPN using Basic DVCP (Not supported on Firebox 500 unless you purchase the BOVPN Upgrade. Supported on Firebox X700, Firebox X1000, and Firebox X2500 only if you register the device with LiveSecurity Service.)
- MUVPN
- RUVPN with PPTP

Regardless of whether the IP settings are stable, 1-to-1 NAT and external aliases are not supported when the Firebox is a PPPoE client, and manual IPSec tunnels are not supported when the Firebox is a DHCP or PPPoE client.

Setting Up the Management Station

The management station runs the System Manager software, which displays a real-time monitor of traffic through the firewall, connection status, and tunnel status. In addition, the WatchGuard Security Event Processor (WSEP) receives and stores log messages and issues notifications based on information it receives from the management station.

You can designate any computer on your network as the management station. On the computer you have chosen, install the management software as follows:

1 Insert the WatchGuard System Manager CD-ROM. If the installation wizard does not appear automatically, double-click `install.exe` in the root directory of the CD.

2 Click **Download Latest Software** on the WatchGuard System Manager Installation screen. This launches your Web browser and connects you to the WatchGuard Web site.

If you do not have an Internet connection, you can install directly from the CD-ROM. However, you will not be eligible for support, strong encryption, or VPN features until you activate the LiveSecurity Service.

3 Follow the instructions on the screen to activate your LiveSecurity Service subscription.

4 Download the WatchGuard System Manager software. Download time will vary depending on your connection speed.

Make sure you write down the name and path of the file as you save it to your hard drive!

5 Execute the file you downloaded and follow the screens to guide you through the installation.

The Setup program includes a screen in which you select software components or upgrades to be installed. Certain components require a separate license.
For more information on the WebBlocker Server option, see Chapter 15, "Controlling Web Site Access." For more information on other components or upgrades, see the WatchGuard Web site.

6 At the end of the installation wizard, a checkbox appears asking if you want to launch the QuickSetup Wizard. You must first cable the Firebox before launching the QuickSetup Wizard.

Another checkbox asks if you want to download a new WebBlocker database. You can download the database either now or later. For more information on the WebBlocker database, see Chapter 15, "Controlling Web Site Access."

Software encryption levels

The management station software is available in three encryption levels.

Base
Uses 40-bit encryption

Medium
Uses 56-bit DES encryption

Strong
Uses 128-bit 3DES encryption

The IPSec standard requires at least a 56-bit encryption. If you want to use virtual private networking with IPSec or PPTP, you must download the strong encryption software.

High encryption software is governed by strict export restrictions and may not be available for download. For more information, see the online support resources at:
https://www.watchguard.com/support/AdvancedFaqs/bovpn_ipsecgrey.asp

(You may be prompted to log in first.)

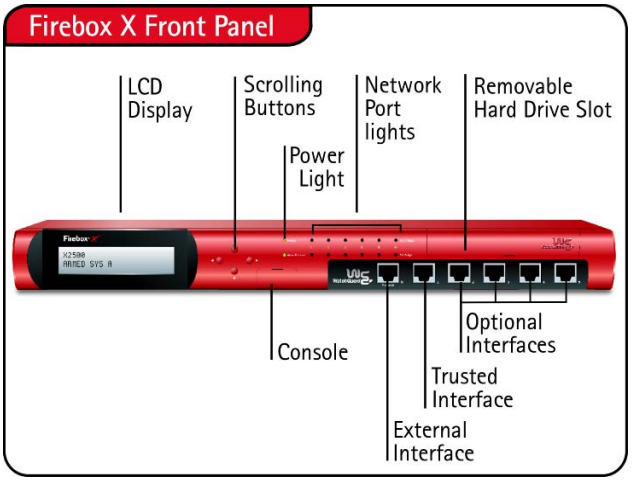
Cabling the Firebox

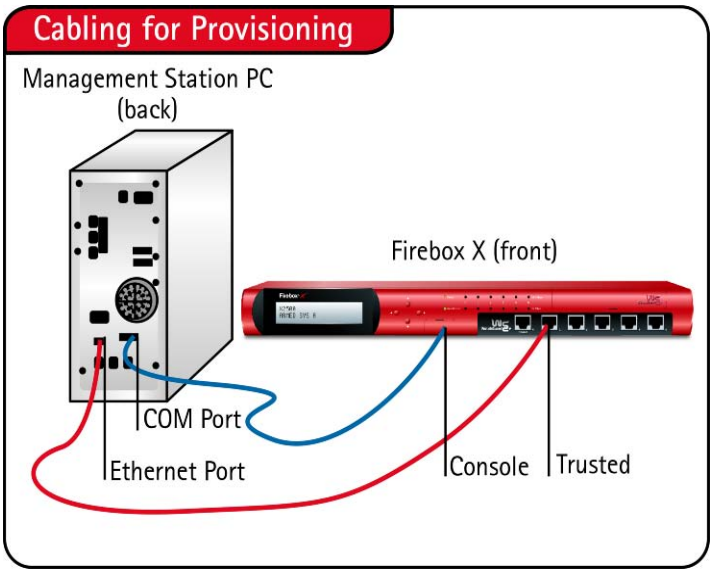
Cable the Firebox to the management station using a serial cable or over a network using TCP/IP. The recommended way is using a serial cable.

Using a serial cable

Refer to the Firebox X Front Panel and Cabling for Provisioning images on the next page when cabling the Firebox.

- Use the blue serial cable to connect the Firebox Serial Port (CONSOLE) to the management station COM port.
- Use the red crossover cable to connect the Firebox trusted interface to the management station Ethernet port.
- Plug the power cord into the Firebox power input and into a power source.





Using TCP/IP

- Use the red (crossover) cable to connect the Firebox trusted interface to the management station Ethernet port.

- Plug the power cord into the Firebox power input and into a power source.

Running the QuickSetup Wizard

After you finish setting up the management station and cabling the Firebox, use the QuickSetup Wizard to create a basic configuration file. The Firebox loads this primary configuration file when it boots. This enables the Firebox to function as a simple but immediately effective firewall.

The QuickSetup Wizard also writes a basic configuration file called `wizard.cfg` to the hard disk of the management station. If you later want to expand or change the basic Firebox configuration using Policy Manager, use `wizard.cfg` as the base file to which you make changes. For more information on changing a configuration file, see Chapter 5, "Using Policy Manager to Configure Your Network." You can also run the QuickSetup Wizard again at any time to a create new, basic configuration file.

NOTE

Rerunning the QuickSetup Wizard completely replaces the configuration file, writing over any prior version. To make a backup copy of the configuration file on the flash disk, see the Firebox System Area chapter in the *Reference Guide*.

If the QuickSetup Wizard is not already launched, launch it from the Windows desktop by selecting **Start ⇒ Programs ⇒ WatchGuard ⇒ QuickSetup Wizard**.

Provide the information as prompted by the QuickSetup Wizard, referring to the tables and network diagrams in "Gathering Network Information" on page 22.

The QuickSetup Wizard takes you through the following steps:

Select a configuration mode

Specify whether you want a routed or a drop-in configuration mode. If you have High Availability installed, it is recommended that you set this up using Policy Manager instead of the QuickSetup Wizard. For more information on routed or drop-in, see "Selecting a Firewall Configuration

Mode" on page 25. For information on High Availability, see the High Availability Guide.

External interface configuration
(Routed configuration only.) Specify static, DHCP, or PPPoE, as explained in "Dynamic IP support on the external interface" on page 30.

Enter the Firebox interface IP address or addresses
Based on whether you specified routed or drop-in mode, enter the IP address or addresses for the Firebox interfaces. You can also add a secondary network to your trusted interface by selecting the **additional private network behind the Firebox** checkbox.

Enter the Firebox Default Gateway
(Not applicable if using DHCP or PPPoE on the external interface.) Enter the IP address of the default gateway, which is usually the IP address of your Internet router. This IP address must be on the same network as the Firebox external interface. If the IP address is not on the same network, the QuickSetup Wizard will warn you and ask whether you want to continue.

Configure Public Servers
(Not applicable if using DHCP or PPPoE on external interface.) Select the checkbox and enter the IP address of any public servers on your network.

Firebox Name
(DHCP or PPPoE only.) Specify the name used for logging and identification of a dynamic Firebox. All characters are allowed except blank spaces and forward or back slashes (/ or \). This name does not have to be a DNS or host name.

Create Passphrase
Passphrases are case-sensitive and must be at least seven characters long. They can be any combination of letters, numbers, and special characters. You will create two passphrases. The status passphrase is used to establish a read-only connection to the Firebox. The configuration passphrase is used to establish a read/write connection to the Firebox.

Select Connection Method

Select the cabling method used and enter a temporary IP address for the Firebox so that the management station can communicate with it to finish the installation process. This must be an unused IP address on the same network as the management station.

Testing the connection

After you have completed the QuickSetup Wizard, test the connection to the Firebox through the management station. The Firebox temporary IP address needs to be on the same network as the management station. If not, the management station and Firebox cannot communicate, and you will not be able to use the management station software to view the Firebox activity.

You can remove the blue serial cable from the management station and Firebox after the QuickSetup Wizard is completed.

Entering IP addresses

You generally enter IP addresses into fields that resemble the one below.



When typing IP addresses, type the digits and periods in sequence. Do not use the TAB key, arrow key, spacebar, or mouse to jump past the periods. For example, if you are typing the address 172.16.1.10, do not type a space after you type "16" or try to position your cursor past the next period to begin typing "1." Instead, type a period right after "16," and then type "1.10." Press the slash (/) key to move to the netmask.

Use slash notation to enter the netmask. In slash notation, a single number indicates how many bits of the IP address identify the network that the host is on. A netmask of 255.255.255.0 has a slash equivalent of 8+8+8=24. For example, writing 192.168.42.23/24 is the same as specifying an IP address of 192.168.42.23 with a corresponding netmask of 255.255.255.0. The following table shows network masks and slash equivalents.

Network mask	Slash equivalent
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Deploying the Firebox into Your Network

Congratulations! You have completed the installation of your Firebox. The Firebox can now be used as a basic firewall with the following properties:

- All outgoing traffic is allowed.
- All incoming traffic is blocked except `ping` on the external interface.
- Logs are sent to the WatchGuard Security Event Processor on the management station.

Complete the following steps to deploy the Firebox into your network:

- Place the Firebox in its permanent physical location.
- Connect the Firebox to your network.
- If using a routed configuration, change the default gateway setting on all desktops to the Firebox trusted IP address.

What's Next

You have successfully installed, configured, and deployed your new WatchGuard System Manager on your network. Here are some things to remember as a new customer.

Customizing your security policy

Your organization's security policy defines who can get into your network, where they can go, and who can get out. The security policy is enacted by your Firebox's configuration file.

The configuration file you created using the QuickSetup Wizard is only a basic configuration. You should now create a configuration file that meets the requirements of your security policy. You do this by adding filtered and proxied services, in addition to the basic ones described in the previous section, that expand what you allow in and out of your firewall.

Every service brings trade-offs between network security and accessibility. When selecting services, balance the needs of your organization with the requirement that computer assets be protected from attack. Some common services that organizations typically add, in addition to the ones listed in the previous section, are HTTP (Internet service) and SMTP (email service). Generally, in a new setup, it is recommended that you use only filtered services until all your system are functional, and then move to proxies as you become familiar with them, as needed.

For more information on services, see Chapter 8, "Configuring Filtered Services", and Chapter 9, "Configuring Proxied Services."

What to expect from LiveSecurity® Service

Your Firebox includes a subscription to our award-winning LiveSecurity Service. Your subscription today:

- Ensures up-to-date network protection with the latest software upgrades.
- Solves problems with comprehensive technical support resources.
- Prevents downtime with alerts and configuration tips to combat the newest threats and vulnerabilities.
- Develops your expertise with detailed interactive training resources.
- Extends your network security with bundled software, utilities, and special offers.

CHAPTER 4

Firebox Basics

This chapter describes the basic tasks you perform to set up and maintain a Firebox:

- Opening a configuration file
- Saving a configuration file to a local computer or the Firebox
- Resetting Firebox passphrases
- Setting the Firebox time zone
- Setting a Firebox friendly name

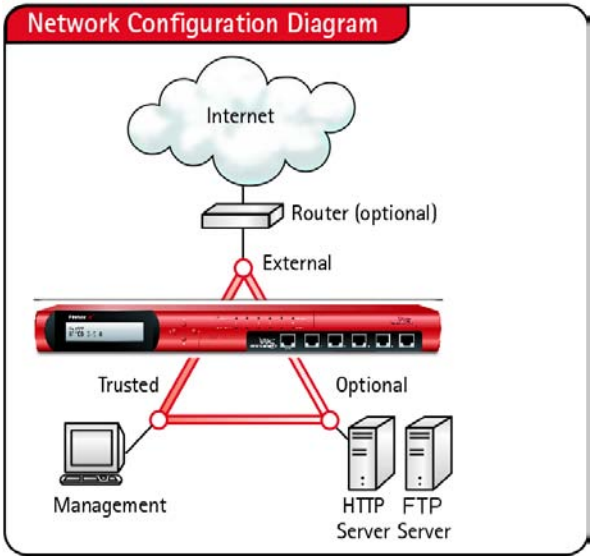
What is a Firebox?

A WatchGuard Firebox is a specially designed and optimized security appliance. The base model has three independent network interfaces which allow you to separate your protected office network from the Internet while providing an optional public interface for hosting Web, email, or FTP servers. Each network interface is independently monitored and visually displayed on the front of the Firebox.

NOTE

There are no user-serviceable parts within the Firebox. If a user opens a Firebox case, it voids the limited hardware warranty.

The most common and effective location for a Firebox is directly behind the Internet router, as pictured below:



Other parts of the network are as follows:

Management station
The computer on which you install and run the WatchGuard System Manager software.

WatchGuard Security Event Processor
The computer that receives and stores log messages and sends alerts and notifications. You can configure the management station to also serve as the event processor.

Trusted network
The network behind the firewall that must be protected from the security challenge.

External network
The network presenting the security challenge, typically the Internet.

Optional network or networks
Networks protected by the firewall but still accessible from the trusted and the external networks. Typically, optional networks are used for public servers such as an FTP or Web server.

Opening a Configuration File

Policy Manager is a comprehensive software tool for creating, modifying, and saving configuration files. A configuration file, with the extension `.cfg`, contains all the settings, options, addresses, and other information that constitute your Firebox security policy. When you view the settings in Policy Manager, you are seeing a "user friendly" version of your configuration file.

This section describes how to open a configuration file after one has been created. This assumes you have already run the Quick-Setup Wizard and have a basic configuration file saved either on the Firebox or on your local hard drive. If you have not run the QuickSetup Wizard, see Chapter 5, "Using Policy Manager to Configure Your Network" for information on how to create a basic configuration from scratch.

1 Select **Start** ⇒**Programs** ⇒**WatchGuard** ⇒**Firebox System Manager**.

2 If you are prompted to run the QuickSetup Wizard, click **Continue**.

3 If you are prompted to connect to the Firebox, click **Cancel**.

4 From the Firebox Manager, click the Policy Manager icon (shown at right).



You can now either open a configuration from the Firebox or from the local hard disk, as explained in the next two sections.

Opening a configuration from the Firebox

From Policy Manager:

1 Select **File** ⇒ **Open** ⇒ **Firebox**.
The Firebox drop-down list, as shown in the following figure, appears.



2 Use the **Firebox** drop-down list to select a Firebox.
You can also type in the IP address or host name.

3 In the **Passphrase** text box, type the Firebox status (read-only) passphrase. Click **OK**.
Use the status passphrase unless you are saving to the Firebox, which requires the configuration passphrase.

4 If you want, enter a value in the **Timeout** field to specify the duration in seconds that the management station waits for a response from the Firebox before returning a message indicating that the device is unreachable.

Opening a configuration from a local hard disk

1 Select **File** ⇒ **Open** ⇒ **Configuration File**.

2 Locate and select the configuration file to open. Click **Open**.

Saving a Configuration File

After making changes to a configuration file, you can either save it directly to the Firebox or to a local hard disk. When you save a new configuration directly to the Firebox, Policy Manager might prompt you to reboot the Firebox so that it will use the new configuration. If the Firebox does need to be rebooted, the new policy is not active until the rebooting process completes.

Saving a configuration to the Firebox

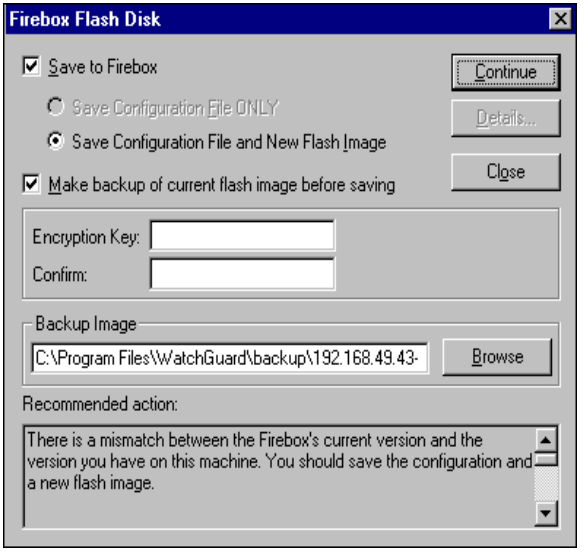
From Policy Manager:

1 Select **File ⇒Save ⇒To Firebox**.
You can also use the shortcut Ctrl+T.

2 Use the **Firebox** drop-down list to select a Firebox.
You can also type the IP address or DNS name of the Firebox. When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

3 Enter the configuration (read/write) passphrase. Click **OK.**
The configuration file is saved first to the local hard disk and then to the primary area of the Firebox flash disk. This is the reason you are prompted to save and to overwrite the existing configuration when saving to the Firebox.

4 If you entered the IP address of a different Firebox, you are asked to confirm your choice. Click **Yes**.
The Firebox Flash Disk dialog box, as shown in the following figure, appears.


Firebox Flash Disk
Save to Firebox
Save Configuration File ONLY
Save Configuration File and New Flash Image
Make backup of current flash image before saving
Continue
Details...
Close
Encryption Key:
Confirm:
Backup Image
C:\Program Files\WatchGuard\backup\192.168.49.43-
Browse
Recommended action:
There is a mismatch between the Firebox's current version and the version you have on this machine. You should save the configuration and a new flash image.

5 Select the checkbox marked **Save To Firebox.** If you want to make a backup of the current image, select the checkbox marked **Make Backup of Current Flash Image before saving.**

NOTE

It is not necessary to back up the flash image every time you make a change to the configuration file. However, if you do choose this option, you must provide an encryption key. It is especially important not to forget this key. If you rely on this file to recover from a corrupted flash image and do not remember the key, you will not be able to restore the entire flash image. Instead, you will need to reset the Firebox and then save a new or existing configuration file to it.

6 If you are not making a backup, click **Continue**. If you are making a backup, in the **Encryption Key** field, enter the encryption key for the Firebox. In the **Confirm** field, reenter it to confirm.

7 If you are making a backup, in the **Backup Image** field, enter the path where you want to save the backup of the current flash image. Click **Continue**.
Instead of entering the path, you can click Browse to specify the location of the backup.

8 Enter and confirm the status (read-only) and configuration (read/write) passphrases. Click **OK**.
The new image is saved to the Firebox.

NOTE

Making routine changes to a configuration file does not require a new flash image. Choosing the option marked Save Configuration File Only is normally sufficient.

Saving a configuration to the management station's local drive

From Policy Manager:

1 Select **File** ⇒ **SaveAs** ⇒ **File**.
You can also use the shortcut Ctrl+S.
The Save dialog box appears.

2 Enter the name of the file.
The default is to save the file to the WatchGuard directory.

3 Click **Save**.
The configuration file is saved to the local hard disk.

Resetting Firebox Passphrases

WatchGuard recommends that you periodically change the Firebox passphrases for optimum security. To do this, you must have the current configuration passphrase. From Policy Manager:

1 Open the configuration file running on the Firebox.
For more information, see "Opening a configuration from the Firebox" on page 44.

2 Select **File ⇒Save ⇒To Firebox**.

3 Use the **Firebox** drop-down list to select a Firebox or enter the Firebox IP address. Enter the configuration passphrase. Click **OK**.
The Firebox Flash Disk dialog box appears.

4 Select the checkbox marked **Save To Firebox** and the radio button marked **Save Configuration File and New Flash Image**. Clear the checkbox marked **Make Backup of Current Flash Image**. Click **Continue**.

5 Enter and confirm the new status (read-only) and configuration (read/write) passphrases. The status and configuration passphrases must be different from one another. Click **OK**.
The new image, including the new passphrases, is saved to the Firebox, and the Firebox automatically restarts.

Tips for creating secure passphrases

Although a persistent attacker can crack any passphrase eventually, you can toughen your passphrases using the following tips:

- Don't use words in standard dictionaries, even if you use them backward or in a foreign language. Create your own acronyms instead.
- Don't use proper names, especially company names or those of famous people.
- Use a combination of uppercase and lowercase characters, numerals, and special characters (such as lm4e@tiN9).

Setting the Firebox Model

Although you choose the Firebox model when you start a new configuration file or open an existing one, you can change the Firebox model at any time:

1 From the **Setup** menu, select **Firebox Model**.
The New Firebox Configuration dialog box appears.

2 Select the model of the Firebox you are connecting to.
The model of the Firebox entered appears at the lower-right corner of the Policy Manager window.

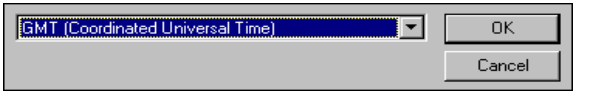
Setting the Time Zone

The Firebox time zone determines the date and time stamp that appear on logs and that are displayed by services such as Log-Viewer, Historical Reports, and WebBlocker. The default time zone is Greenwich Mean Time (Coordinated Universal Time).

From Policy Manager:

1 Select **Setup** ⇒ **Time Zone**.

2 Use the drop-down list to select a time zone. Click **OK**.



Setting a Firebox Friendly Name

You can give the Firebox a friendly name to be used in log files and reports. If you do not specify a name, the Firebox's IP address is used. From Policy Manager:

1 Select **Setup** ⇒ **Name**.
The Firebox Name dialog box appears.

2 Enter the friendly name of the Firebox. Click **OK**.
All characters are allowed except blank spaces and forward or back slashes (/ or \).



This is typically set to the external IP address of the Firebox. If left blank, some features may fail to function properly.

CHAPTER 5

Using Policy Manager to Configure Your Network

Normally, you incorporate the Firebox into your network when you run the QuickSetup Wizard, as described in "Running the QuickSetup Wizard" on page 35. However, you can also create a basic configuration file from scratch using several functions in Policy Manager.

Each of the procedures in this section can also be used to override any settings you made using the QuickSetup Wizard. It is recommended that you follow these steps in the following order to make sure that all necessary information is provided (although not all steps are required in all installations).

- Starting a new configuration file
- Setting up Firebox interfaces
- Adding secondary networks
- Defining DNS and WINS servers on your network
- Setting up the Firebox as a DHCP server
- Adding the four basic services to Policy Manager
- Configuring routes, if WAN routers are behind the Firebox reaching other networks

Starting a New Configuration File

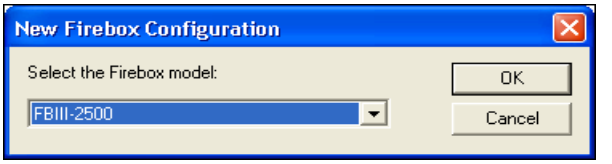
To start a new configuration file:

1 From System Manager, click the Policy Manager button, shown at right.
Policy Manager appears.



2 From Policy Manager, select **File ⇒ New**.

3 From the **New Firebox Configuration** dialog box, select the model of Firebox you are connected to.



The new configuration file contains defaults for the model of Firebox specified.

Setting the Firebox Configuration Mode

For information on routed and drop-in configurations, see “Selecting a Firewall Configuration Mode” on page 25.

You must decide upon your configuration mode before setting IP addresses for the Firebox interfaces. If you specify an incorrect IP address, you may run into problems later.

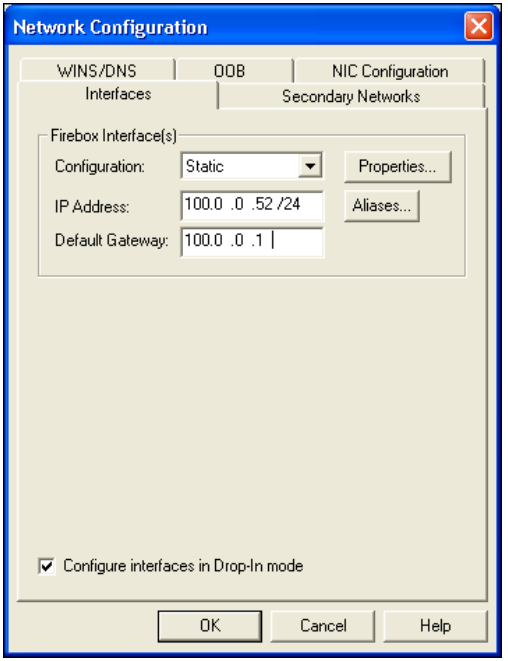
Setting IP Addresses of Firebox Interfaces

The way you set the IP addresses for the Firebox interfaces depends on the configuration mode you have chosen.

Setting addresses in drop-in mode

If you are using drop-in mode, all interfaces use the same IP address:

1 Select **Network ⇒ Configuration**.
The Network Configuration dialog box appears, as shown in the following figure.



2 Select the **Configure interfaces in Drop-In mode** checkbox, located at the bottom of the dialog box.

3 Enter the IP address and default gateway for the Firebox interfaces.

When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

If you are using static PPPoE on your external interface, you also need to enter your PPP user name and password. For more information on PPPoE support, see "Dynamic IP support on the external interface" on page 30.

4 Select the method for obtaining an IP address: **Static**, **DHCP**, or **PPPoE**.

Setting addresses in routed mode

If you are using routed mode, the interfaces must use different IP addresses. At least two interfaces must have IP addresses configured.

1 Select **Network ⇒ Configuration**.
The Network Configuration dialog box appears.

2 For each interface, in the **IP Address** text box, type the address in slash notation.
When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

3 For the external interface, enter the default gateway.

Setting DHCP or PPPoE Support on the External Interface

For information on the DHCP and PPPoE options, see "Dynamic IP support on the external interface" on page 30.

1 Select **Network ⇒ Configuration**.
The Network Configuration dialog box appears.

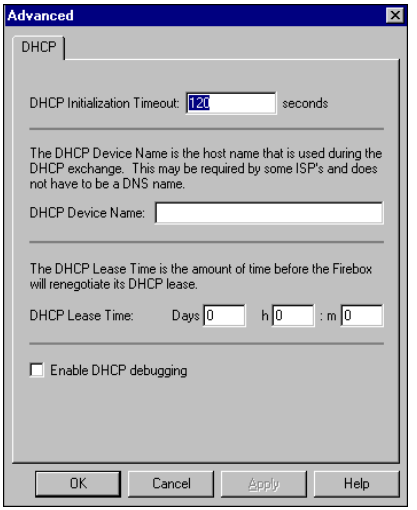
2 Select either **DHCP** or **PPPoE** from the **Configuration** drop-down list.

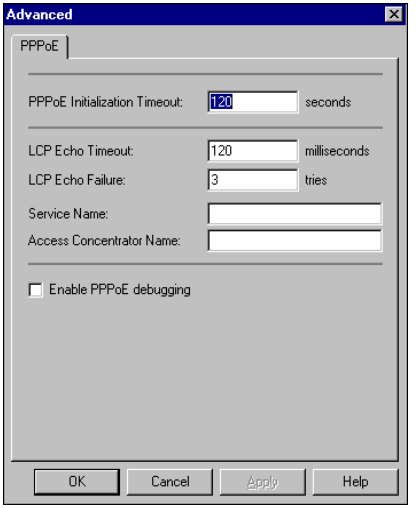
3 If you enabled PPPoE support, enter the PPP user name and password in the fields provided.

Configuring DHCP or PPPoE support

If you enable DHCP or PPPoE on the external interface, you can set several optional properties:

1 From the **Network Configuration** dialog box, click **Properties**.
The Advanced dialog box appears, showing the DHCP or PPPoE tab, as shown in the following figures.


Advanced
DHCP
DHCP Initialization Timeout: 120 seconds
The DHCP Device Name is the host name that is used during the DHCP exchange. This may be required by some ISP's and does not have to be a DNS name.
DHCP Device Name:
The DHCP Lease Time is the amount of time before the Firebox will renegotiate its DHCP lease.
DHCP Lease Time: Days 0 h 0 : m 0
Enable DHCP debugging
OK
Cancel
Apply
Help



2 Set an initialization timeout in the **DHCP Initialization Timeout** field.

3 In the **DHCP Device Name** field, assign a name to the device.

The name can be any combination of ASCII numbers and letters up to 15 characters in length, but spaces are not allowed. It is preferable to use a name that does not identify the unit as a Firebox

or SOHO. Examples of recommended names are PC1003 or HomeOffice. Examples of names that are not recommended are Firebox2 or SOHO6Alpha.

NOTE

PPPoE debugging generates large amounts of data. Do not enable PPPoE debugging unless you are having connection problems and need help from Technical Support.

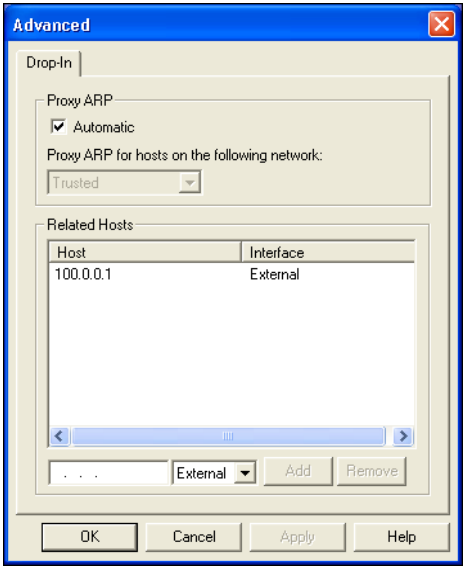
Enabling static PPPoE

Although an IP address is generally obtained automatically when using PPPoE, static PPPoE is also supported. To enable static PPPoE, click **Use the following IP address**, and then enter the IP address and default gateway.

Configuring Drop-in Mode

If you selected drop-in mode, you can set several optional properties:

1 From the **Network Configuration** dialog box, click **Properties**.
The Advanced dialog box appears, showing the Drop-In tab, as shown in the following figure.



2 Configure the properties in the dialog box.
For a description of each control, right-click it and then select What's This?.

Defining External IP Aliases

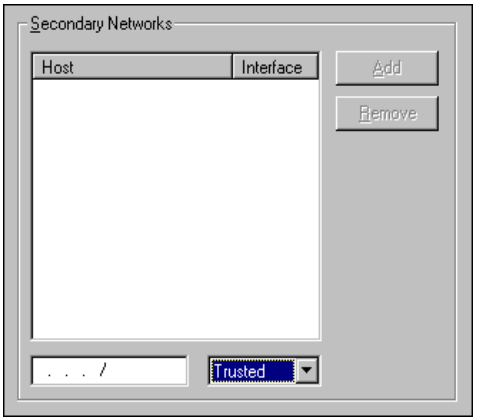
You use the **Aliases** button on the **Network Configuration** dialog box when you are using static NAT. For more information, see “Adding external IP addresses” on page 101.

Adding Secondary Networks

Your configuration may require that you add secondary networks to any of the Firebox interfaces. For more information on secondary networks, see “Adding secondary networks to your configuration” on page 29.

1 Select **Network** ⇒ **Configuration**.
The Network Configuration dialog box appears.

2 Click the **Secondary Networks** tab.
The Secondary Networks tab appears, as shown in the following figure.



3 Use the drop-down list in the lower-right portion of the dialog box to select the interface to which you want to add a secondary network.

4 Use the field in the lower-left portion of the dialog box to type an unused IP address from the secondary network.
When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

NOTE

Check secondary network addresses carefully. Policy Manager does not verify that you have entered the correct address. WatchGuard strongly recommends that you do not enter a subnet on one interface that is part of a larger network on another interface or route. Spoofing can occur and the network will not function properly.

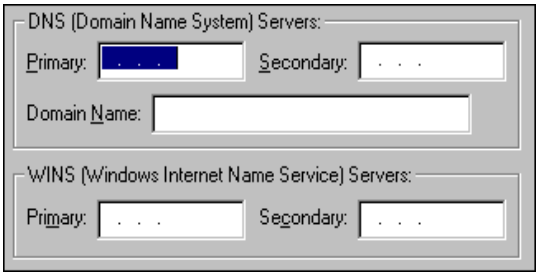
Entering WINS and DNS Server Addresses

Several advanced features of the Firebox, such as DHCP and Remote User VPN, rely on shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. These servers must be accessible from the Firebox trusted interface.

Make sure you use only an internal DNS server for DHCP and Remote User VPN. Do not use external DNS servers.

From Policy Manager:

1 Select **Network** ⇒ **Configuration**. Click the **WINS/DNS** tab.
The WINS/DNS tab appears, as shown in the following figure.



2 Enter primary and secondary addresses for the WINS and DNS servers. Enter a domain name for the DNS server.

Configuring Out-of-Band Management

You use the **OOB** tab on the **Network Configuration** dialog box to enable the management station to communicate with a Firebox by way of a modem (not provided with the Firebox) and telephone line. For information on configuring out-of-band management, see Chapter 16, "Connecting with Out-of-Band Management."

Defining a Firebox as a DHCP Server

Dynamic Host Configuration Protocol (DHCP) is an Internet protocol that simplifies the task of administering a large network. A device defined as a DHCP server automatically assigns IP addresses to network computers from a defined pool of numbers. You can define the Firebox as a DHCP server for the customer network behind the firewall.

NOTE

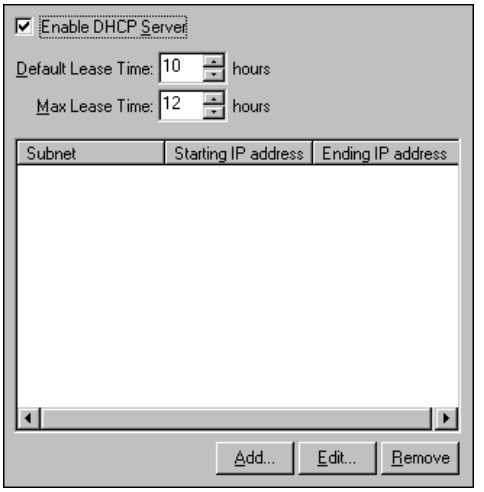
If you have a larger network with a domain controller, WatchGuard recommends that you configure the domain controller to provide DHCP services.

One parameter that you define for a DHCP server is lease times. This is the amount of time a DHCP client can use an IP address that it receives from the DHCP server. When the time is close to expiring, the client contacts the DHCP server to renew the lease.

Note that the Firebox should not be used to replace an enterprise DHCP server. If you already have a DHCP server configured, you should continue to use that server for DHCP.

From Policy Manager:

1 Select **Network** ⇒ **DHCP Server**.
The DHCP Server dialog box appears, as shown in the following figure.



2 Select the **Enable DHCP Server** checkbox.

3 Enter the default lease time for the server.
The default lease time is provided to clients that do not specifically request times.

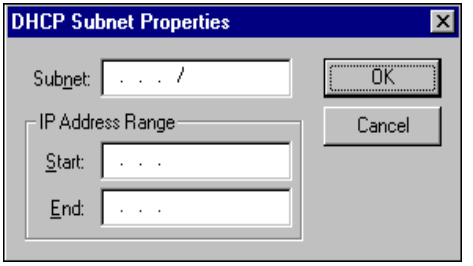
4 Enter the maximum lease time.
The maximum lease time is the longest time the server will provide for a client. If a client requests a longer time, the request is denied and the maximum lease time is provided.

Adding a new subnet

To make available (private) IP addresses accessible to DHCP clients, add a subnet. To add a new subnet, you specify a range of IP addresses to be assigned to clients on the network. For example, you could define the address range from 10.1.1.10 to 10.1.1.19 to give clients a pool of 10 addresses. From Policy Manager:

1 Select **Network** ⇒ **DHCP Server**.

2 Click **Add**.
The DHCP Subnet Properties dialog box appears, as shown in the following figure.



3 In the **Subnet** box, type the subnet's IP address; for example, 10.1.1.0/24.

4 Define the address pool by entering values for **Start** and **End** fields.

5 Click **OK**.

Modifying an existing subnet

You can modify an existing subnet; however, you should be aware that doing so can cause problems. If you modify the subnet and then reboot the client, the Firebox may return an IP address that does not work with certain devices or services.

From Policy Manager:

1 Select **Network** ⇒ **DHCP Server**.

2 Click the subnet to review or modify. Click **Edit**.

3 The **DHCP Subnet Properties** dialog box appears.

4 When you have finished reviewing or modifying the subnet, click **OK**.

Removing a subnet

You can remove an existing subnet; however, you should be aware that doing so can cause problems. If you remove the subnet and then reboot the client, the Firebox may return an IP address that does not work with certain devices or services.

From Policy Manager:

1 Select **Network** ⇒ **DHCP Server**.

2 Click the subnet to remove it. Click **Remove**.

3 Click **OK**.

Adding Basic Services to Policy Manager

After you have set up IP addressing, add the following services to Policy Manager to give your Firebox some basic functionality.

NOTE

The WatchGuard service is particularly important. If you omit it from your configuration or misconfigure it, you will lock yourself out of the Firebox.

1 On the Policy Manager toolbar, click the Add Services icon (shown at right).



2 Click the plus (+) sign to the left of the **Packet Filters** and **Proxies** folders to expand them.
A list of pre-configured filters or proxies appears.

3 Under **Packet Filters,** click **WatchGuard**.

4 Click the **Add** button at the bottom of the dialog box.

5 Click **OK** in the **Add Service** dialog box.

6 Click **OK** to close the **Properties** dialog box.

7 Repeat steps 3–6 for the Ping, FTP, and Outgoing services.

At this stage, do not change the default settings for any of these basic services. The default settings allow all traffic outbound and deny all traffic inbound. Later, you can go back and modify the services in Policy Manager to best fit your security needs.

If you need more detailed information on how to add services, see “Adding a service” on page 111.

Configuring Routes

A route is the sequence of devices that network traffic takes from its source to its destination. A router is a device within a route that determines the next point to which traffic should be forwarded toward its destination. Each router is connected to at least two networks. A packet may travel through a number of network points with routers before arriving at its destination.

The Firebox supports the creation of static routes in order to pass traffic from any of its three interfaces to a router. The router can then pass traffic to the appropriate destination according to its specific routing policies.

For more information on routing issues, see the following FAQ: https://www.watchguard.com/support/AdvancedFaqs/general_routers.asp

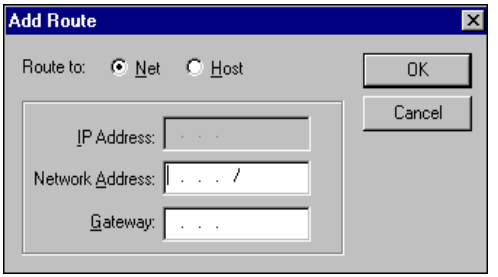
The WatchGuard user's forum is also a good source of information on routing information. Log in to your LiveSecurity account for more details.

Defining a network route

Define a network route if you have an entire network behind a router that resides on your local network. Enter the network IP address, including slash notation. From Policy Manager:

1 Select **Network** ⇒ **Routes**.
The Setup Routes dialog box appears.

2 Click **Add**.
The Add Route dialog box appears, as shown in the following figure.



3 Click the **Net** option.

4 Enter the network IP address.

5 In the **Gateway** text box, enter the IP address of the router.
Be sure to specify an IP address that is on one of the same networks as the Firebox.

6 Click **OK**.
The Setup Routes dialog box lists the newly configured network route.

7 Click **OK**.
The route data is written to the configuration file.

Defining a host route

Define a host route if there is only one host behind the router. Enter the IP address of that single, specific host, without slash notation. From Policy Manager:

1 Select **Network ⇒ Routes**.
The Setup Routes dialog box appears.

2 Click **Add**.
The Add Route dialog box appears.

3 Click the **Host** option.

4 Enter the host IP address.

5 In the **Gateway** text box, enter the IP address of the router.
Be sure to specify an IP address that is on one of the same networks as the Firebox.

6 Click **OK**.
The Setup Routes dialog box lists the newly configured host route.

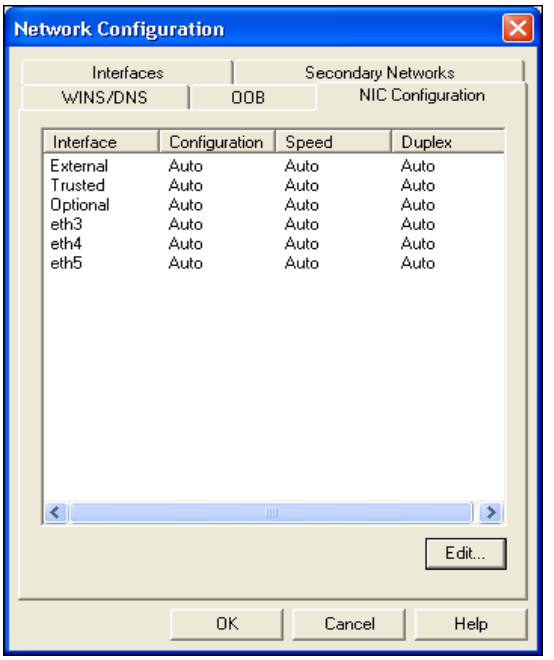
7 Click **OK**.
The route data is written to the configuration file.

Specifying Manual or Automatic Settings for Ports

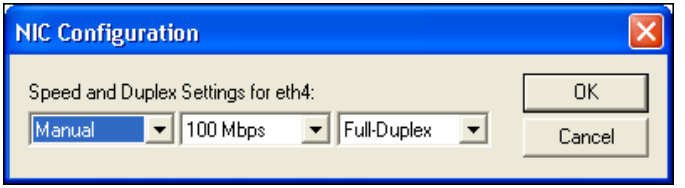
You can specify whether the speed and duplex settings for Firebox ports are automatically set or user configurable. WatchGuard recommends using the Auto setting.

1 Select **Network ⇒ Configuration**.
The Network Configuration dialog box appears.

2 Select the **NIC Configuration** tab.
The NIC Configuration dialog box appears.



3 The current settings appear on the screen. To change them, select the port you want to change and click **Edit**.



4 From the drop-down list, select either **Auto** or **Manual**. If you select **Manual**, select the speed you want and either half-duplex or full-duplex.

CHAPTER 6

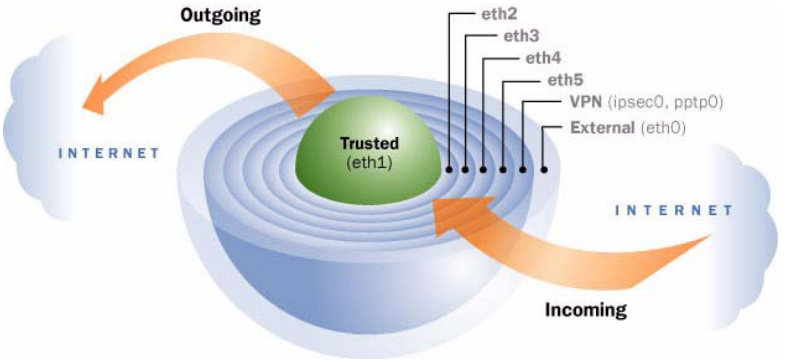
Managing and Monitoring the Firebox

WatchGuard System Manager combines access to several security applications and tools in one intuitive interface. System Manager also includes a real-time monitor of traffic through the firewall, as well as a number of monitoring tools.

This chapter also describes HostWatch, an application that provides a real-time display of active connections on a Firebox.

About Incoming and Outgoing Traffic

Network traffic is classified as either incoming or outgoing. The following conceptual figure shows the direction of traffic as it relates to all possible Firebox interfaces. Inbound traffic is that which travels toward the core; outbound traffic travels away from the core.



NOTE

This figure assumes you have a Firebox X and have purchased the 3-Port Upgrade to enable the three extra ethernet ports. However, the concepts regarding traffic flow and trust relationships among the different Firebox interfaces apply regardless of whether you have purchased the upgrade.

The distance to the core determines level of trust: the closer to the core of the sphere, the more protected the interface. The least trusted of all source of traffic is the external interface (eth0). All traffic originating from the external interface is incoming traffic, regardless of the destination network behind your Firebox. All traffic destined for the external interface is outgoing traffic, regardless of the location in your organization it originated from.

Conversely, the most trusted source of traffic is the trusted interface (eth1), located at the center of the above diagram. All traffic entering your trusted network is incoming, and all traffic exiting your trusted network is outgoing.

Starting System Manager and Connecting to a Firebox

From the Windows Desktop:

1 Select **Start ⇒Programs ⇒WatchGuard ⇒Firebox System Manager**.

2 If you have not yet configured your Firebox, click **QuickSetup** to start the QuickSetup Wizard, as explained in the QuickStart Guide included with your Firebox. Otherwise, click **Continue**.

The Connect to Firebox dialog box appears. You can connect to a Firebox at this point, or you can cancel the Connect to Firebox dialog box and connect to a Firebox later.

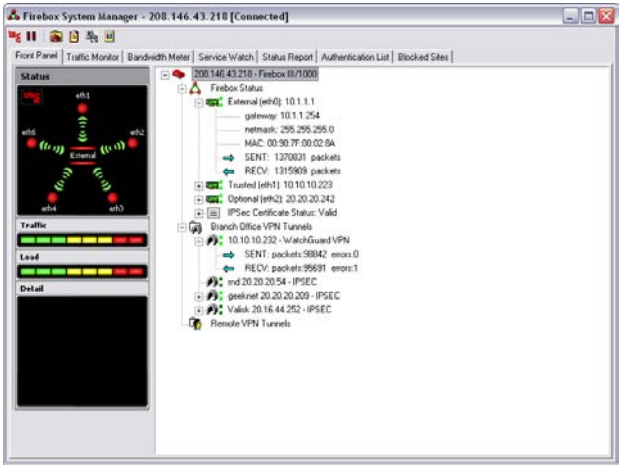
3 If you want to connect to a Firebox at this time, use the **Firebox** drop-down list to select a Firebox.

You can also type the IP address or DNS name of the Firebox. When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

4 Enter the Firebox status (read-only) passphrase.

5 Click **OK**.

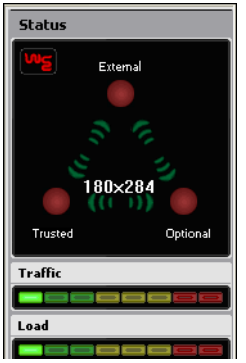
The Front Panel tab of the Firebox System Manager appears, as shown in the following figure.

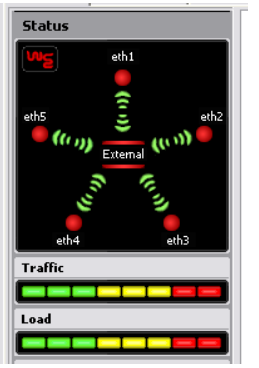


Using the Security Traffic Display

The System Manager initially displays the information shown in the following figure. The security traffic display is an LED indicator on the front of a Firebox that indicates the directions of traffic between the Firebox interfaces. The display can either be

a triangle display (shown below left), for Fireboxes with three interfaces, or a star display (shown below right), for Fireboxes with six interfaces.





To switch between the triangle and the star display, right-click the display and select either **Triangle display** or **Star display**.

Viewing status information

The WatchGuard logo in the upper-left corner of the star or triangle display shows whether the Firebox is connected. If the logo is illuminated, the Firebox is connected; if not, it is not connected.

The “legs” of the star and triangle show traffic flowing through the interfaces. Each leg shows inbound and outbound connections using separate arrows. When there is activity between two interfaces, the arrows pulse in the direction of the traffic.

In the star diagram, the globes at the intersections of the legs can show one of three states:

- dimmed red (idle): there is no traffic beyond that which the legs are displaying.
- red (deny): a connection is being denied on the interface.
- green (allow): there is traffic between this interface and another (but not the center) on the star. When traffic exists between this interface to the center, the leg between these interfaces appears as green pulsing arrows.

In the triangle diagram, the activity is shown in the legs of the triangle. The globes show only the idle or deny states.

Selecting the center interface

If you are using the star display, you can select which interface appears in its center to best represent your network configuration. Point to either the interface name or the globe associated with it, and then click it. The interface then moves to the center of the star. All other interfaces reposition in a clockwise direction.

Basic System Manager Functionality

The top part of the display just below the title bar contains several buttons for performing basic operations and launching WatchGuard System Manager applications:

 Open the main menu for System Manager. (This is also referred to as the Main Menu button.)

 Pause the display (appears only when connected to Firebox)

 Connect to Firebox (appears only when not connected to Firebox)

 Launch Policy Manager

 Launch LogViewer

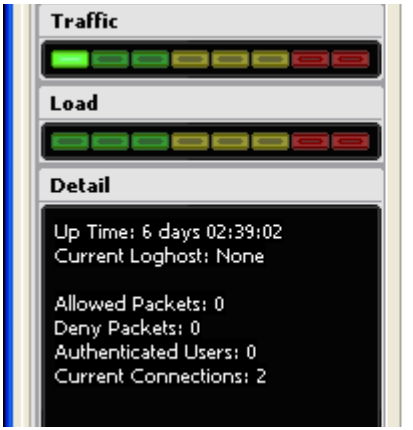
 Launch HostWatch

 Create Historical Reports

For more information on launching these applications, see “Launching Firebox Applications” on page 80.

Viewing basic indicators

Beneath the security traffic display is the traffic volume indicator, processor load indicator, and basic status information.



The two bar graphs indicate traffic volume and the proportion of Firebox capacity being used.

For more information on the front panel, see the following FAQ:
https://www.watchguard.com/advancedfaqs/fbhw_lights.asp

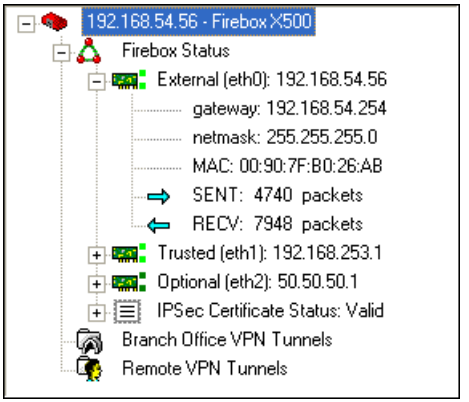
Firebox and VPN tunnel status

The section in System Manager to the right of the front panel shows the current status of the Firebox and of branch office and remote user VPN tunnels.

Firebox Status

The following information is displayed under Firebox Status, as shown in the following figure:

- Status of the High Availability option. When properly configured and operational, the IP address of the standby box appears. If High Availability is installed but the secondary Firebox is not responding, the display indicates “Not Responding.”
- The IP address of each Firebox interface, and the configuration mode of the External interface.
- Status of the CA (root) certificate and the IPSec (client) certificate.



If you expand the entries under Firebox Status, you can view:

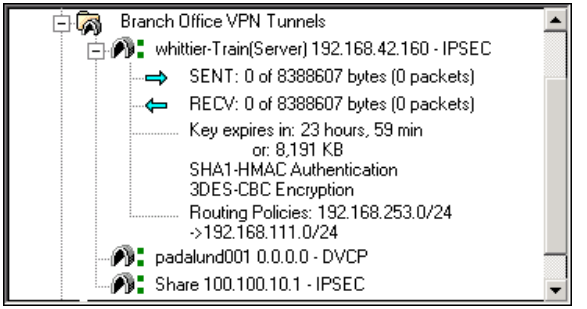
- IP address of the default gateway and netmask.
- MAC (Media Access Control) address of each interface.
- Number of packets sent and received since the Firebox rebooted.
- Expiration date and time of root and IPSec certificates.
- CA fingerprint. This is used to detect man-in-the-middle attacks. For more information, see “Detecting Man-in-the-Middle Attacks” on page 170.

Branch Office VPN Tunnels

Beneath Firebox Status is a section on BOVPN tunnels, in which two categories of these types of tunnels appear: IPSec and DVCP.

The figure below shows an expanded entry for a BOVPN tunnel. The information displayed, from top to bottom, is:

- The name assigned to the tunnel during its creation, along with the IP address of the destination IPSec device (such as another Firebox, SOHO, or SOHO|tc), and the tunnel type (IPSec or DVCP). If the tunnel is DVCP, the IP address refers to the entire remote network address rather than that of the Firebox or equivalent IPSec device.


Branch Office VPN Tunnels
whittier-Train(Server) 192.168.42.160 - IPSEC
SENT: 0 of 8388607 bytes (0 packets)
RECV: 0 of 8388607 bytes (0 packets)
Key expires in: 23 hours, 59 min
or: 8,191 KB
SHA1-HMAC Authentication
3DES-CBC Encryption
Routing Policies: 192.168.253.0/24
->192.168.111.0/24
padalund001 0.0.0.0 - DVCP
Share 100.100.10.1 - IPSEC

- The amount of data sent and received on the tunnel in both bytes and packets.
- The time at which the key expires and the tunnel is renegotiated. Expiration can be expressed as a time deadline or in bytes passed. DVCP tunnels that have been configured for both traffic and time deadline expiration thresholds display both; this type of tunnel expires when either event occurs first (time runs out or bytes are passed).
- Authentication and encryption levels set for the tunnel.
- Routing policies for the tunnel.

Remote VPN Tunnels

Following the branch office VPN tunnels is an entry for remote VPN tunnels, which includes Mobile User VPN (with IPSec) or RUVPN with PPTP tunnels.

If the tunnel is Mobile User VPN, the branch displays the same statistics as for the DVCP or IPSec Branch Office VPN described previously: the tunnel name, followed by the destination IP address, followed by the tunnel type. Below are the packet statistics, followed by the key expiration, authentication, and encryption specifications.

If the tunnel is RUVPN with PPTP, the display shows only the quantity of sent and received packets. Byte count and total byte count are not applicable to PPTP tunnel types.

Expanding and collapsing the display

To expand a branch of the display, click the plus sign (**+**) next to the entry, or double-click the name of the entry. To collapse a branch, click the minus sign (**–**) next to the entry. A lack of

either a plus or minus sign indicates that no further information about the entry is available.

Red exclamation point

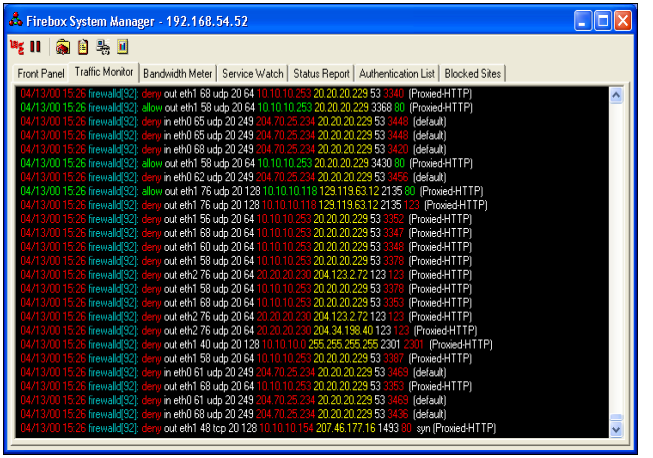
A red exclamation point appearing next to any item indicates that something within its branch is not communicating properly with the Firebox management station. For example, a red exclamation point next to the Firebox entry indicates that a Firebox is not communicating with either the WatchGuard Security Event Processor (WSEP) or management station. A red exclamation point next to a tunnel listing indicates a tunnel is down.

When you expand an entry that has a red exclamation point, another exclamation point appears next to the specific device or tunnel with the problem. Use this feature to rapidly identify and locate problems in your VPN network.

Monitoring Firebox Traffic

To view log messages generated by the Firebox, click the **Traffic Monitor** tab. For more information about messages displayed, see the following collection of FAQs:

https://www.watchguard.com/support/advancedfaqs/log_main.asp



Setting the maximum number of log entries

You can change the maximum number of log entries that are stored and viewable on the Traffic Monitor tab. After the maximum is reached, the earliest logs are removed as more come in. A high value in this field places a large demand on your system if you have a slow processor or a limited amount of RAM. In this situation, LogViewer is a much more appropriate tool for tracking logs than the traffic monitor in System Manager.

1 Click the Main Menu button. Click **Settings**.

2 Type or use the scroll control to change the **Max Log Entries** field. Click **OK**.
The value entered represents the number of logs in thousands. If you enter zero (0) in this field, the maximum number of logs (3,000) is permitted.

Displaying entries in color

You can specify that the log entries appear in different colors according to the type of information they show:

1 Click the Main Menu button. Click **Settings**. Click the **Traffic Monitor** tab.

2 To enable displaying entries in color, select the checkbox marked **Display Logs in Color**.

3 On the **Allow**, **Deny**, or **Message** tab, click the field you want to colorize.
The Text Color field to the right of the tabs shows the current color defined for the field.

4 To change the color, click the arrow next to **Text Color**. Click one of the 20 colors on the palette.
The information contained in this field will appear in the new color on Traffic Monitor. A sample of how the Traffic Monitor will look appears on the bottom of the dialog box.

5 You can also choose a background color for the traffic monitor. Click the arrow next to **Background Color**. Click one of the 20 colors on the palette.

6 To cancel the changes you have made in this dialog box since opening it, click **Reset to Defaults**.

Copying messages to another application

To copy a log message so you can paste it into another application such as email or Wordpad, right-click the message and

select **Copy Selection**. You can then open up the other application and paste in the message.

Copying or analyzing deny messages

You can use several tools to copy and analyze deny messages:

- To copy a deny message and paste it into an application, use the procedure in the previous section.
- To copy the source or destination IP address of a deny message so you can paste it into another application, right-click the message, select **Source IP ⇒ Copy** or **Destination IP ⇒ Copy**.
- To issue the ping command to a source or destination IP address of a deny message, right-click the message and select **Source IP ⇒ Ping** or **Destination IP ⇒ Ping**. (When you issue this command, you are prompted to enter the configuration passphrase.)
- To issue a traceroute command to a source or destination IP address of a deny message, right-click the message and select **Source IP ⇒ Trace Route** or **Destination IP ⇒ Trace Route**. (When you issue this command, you are prompted to enter the configuration passphrase.)

Performing Basic Tasks with System Manager

The basic tasks you perform with System Manager are:

- Running the QuickSetup Wizard
- Flushing the ARP cache
- Connecting to a Firebox
- Changing the interval at which the Firebox is queried for status information
- Getting Help on the Web
- Opening other WatchGuard System Manager applications

Running the QuickSetup Wizard

Normally, you will run the QuickSetup Wizard when you first install your Firebox. However, you can run it from System Manager as well.

1 Click the Main Menu button (shown at right), which is located on the upper-left corner of System Manager.



2 Select **QuickSetup Wizard**.
The QuickSetup Wizard begins. For more information on running the QuickSetup Wizard, see the QuickStart Guide included with your Firebox.

Flushing the ARP cache

The ARP (Address Resolution Protocol) cache on the Firebox stores hardware (MAC) addresses of TCP/IP hosts. This cache is checked for hardware address mapping before an ARP broadcast is initiated. Flushing the ARP cache is important when your network has a drop-in configuration: all trusted computers must have their ARP caches flushed.

To flush out-of-date cache entries:

1 Click the Main Menu button (shown at right). Select **Management ⇒ Flush ARP Cache**.



2 Enter the Firebox configuration (read/write) passphrase.
The out-of-date cache entries are flushed.

Connecting to a Firebox

When launched, System Manager automatically prompts you to connect to the last Firebox with which it established a connection. You can connect to that Firebox or you can specify a different one. From System Manager:

1 Click the Main Menu button (shown at right). Select **Connect**.
The Connect to Firebox dialog box appears.



2 Use the **Firebox** drop-down list to select a Firebox.
You can also type the IP address or DNS name of the Firebox. When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

3 Enter the Firebox status passphrase.

4 Click **OK**.
System Manager connects to the Firebox and displays its real-time status.

Changing the polling rate

You can change the interval of time (in seconds) at which System Manager polls the Firebox and updates the Front Panel and the Firebox and Tunnel Status displays. There is, however, a trade-off between polling frequency and demand on the Firebox. The shorter the interval, the more accurate the display, but also the more demand made of the Firebox.

1 Click the Main Menu button. Click **Settings**.

2 Type or use the scroll control to change the polling rate. Click **OK**.

Getting Help on the Web

You can access additional information about the WatchGuard System Manager from the Firebox System Manager menus. Click the Main Menu button. Click **On the Web**. The menu has the following options:

Homepage
Select to bring up the WatchGuard home page at: http://www.watchguard.com

LiveSecurity Service Logon
Select to log in to the LiveSecurity Service. For more information on this service, see Chapter 2, “Service and Support.”

Training and Certification
Select to bring up the WatchGuard Training and Certificate page at:
http://www.watchguard.com/training/

Activate LiveSecurity Service
Select to activate LiveSecurity Service. For more information on this service, see Chapter 2, “Service and Support.”

Launching Firebox Applications

You launch the following applications from the toolbar at the top of System Manager:

Policy Manager
LogViewer
HostWatch
Historical Reports
WatchGuard Security Event Processor

Launching Policy Manager



Use the WatchGuard Policy Manager tool to design, configure, and manage the network security policy. Within Policy Manager, you can configure networks and services, set up virtual private networking, regulate incoming and outgoing access, and control logging and notification.

Launching LogViewer



The LogViewer application displays a static view of a log file. You can filter by type, search for keywords and fields, and print and save log data to a separate file. For more information, see Chapter 13, “Reviewing and Working with Log Files.”

Launching HostWatch



The HostWatch application displays active connections occurring on a Firebox in real time. It can also graphically represent the connections listed in a log file, either playing back a previous file for review or displaying connections as they are added to the current log file. For more information, see “HostWatch” on page 91.

Launching Historical Reports



Historical Reports is a report-building tool that creates HTML reports displaying session types, most active hosts, most used services, URLs, and other data useful in monitoring and troubleshooting your network. For more information, see “Generating Reports of Network Activity” on page 215.

Opening the WSEP user interface



The WatchGuard Security Event Processor (WSEP) controls logging, report schedules, and notification. It also provides timing services for the Firebox. The WSEP automatically runs when you start the machine on which it is installed.

Unlike other WatchGuard System Manager applications, the WSEP button does not appear in System Manager. To open the WSEP, right-click the WatchGuard Security Event Processor icon (shown above) in the Windows Desktop tray. Click **WSEP Status/ Configuration**. For more information, see "Setting up the WatchGuard Security Event Processor" on page 190.

If the WSEP icon is not displayed in the Windows desktop tray, click the Main Menu button. Select **Tools** ⇒ **Logging** ⇒ **Event Processor Interface**.

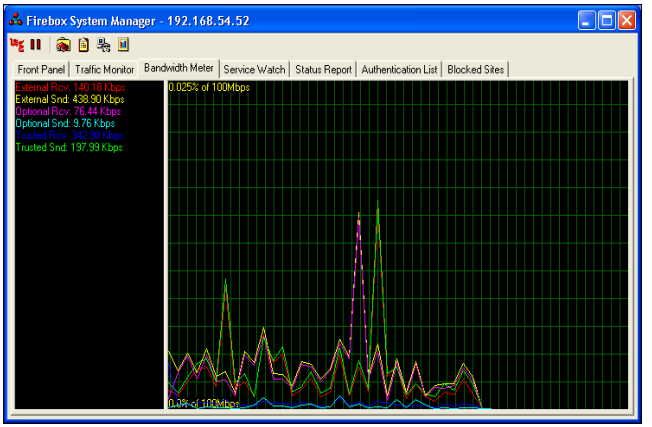
Viewing Bandwidth Usage

Click the **Bandwidth Meter** tab to view real-time bandwidth usage for all Firebox interfaces. The display differentiates by color each interface being graphed.

To configure the colors used on this display:

1 Click the Main Menu button, and select **Settings**.

2 Click the **Bandwidth Meter** tab. Adjust the settings as appropriate.



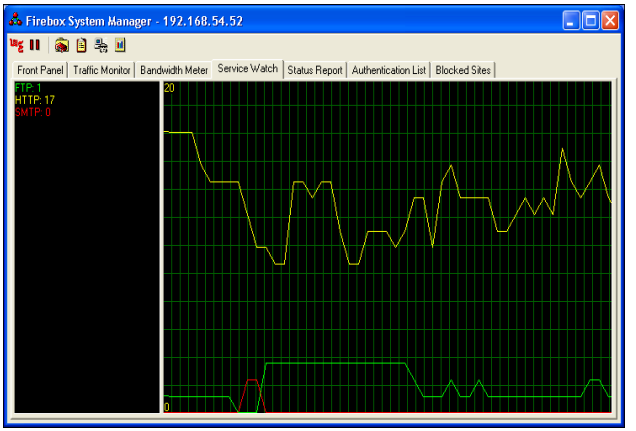
Viewing Number of Connections by Service

The **ServiceWatch** tab on the System Manager display, shown in the following figure, graphs the number of connections by service, providing a service-centric view of network activity. The y axis shows the number of connections and the x axis shows time. The display differentiates by color each service being graphed.

To configure the services that appear and how they are displayed:

1 Click the Main Menu button, and select **Settings**.

2 Click the **Service Watch** tab. Adjust the settings as appropriate.

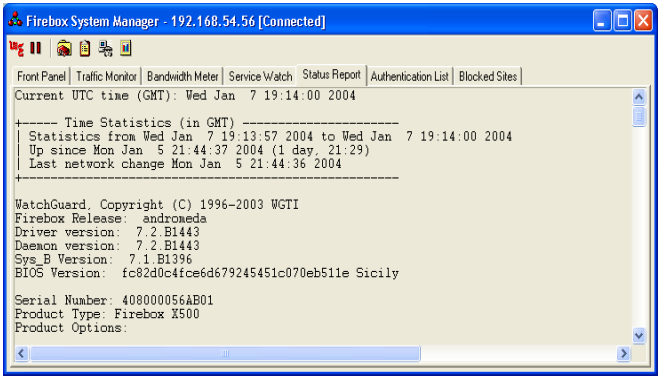


Viewing Details on Firebox Activity

The **Status Report** tab on System Manager provides a number of statistics on Firebox activity.

Firebox uptime and version information

The time range on the statistics, the Firebox uptime, and the WatchGuard System Manager software version.


Firebox System Manager - 192.168.54.56 [Connected]
Front Panel
Traffic Monitor
Bandwidth Meter
Service Watch
Status Report
Authentication List
Blocked Sites
Current UTC time (GMT): Wed Jan 7 19:14:00 2004
+------ Time Statistics (in GMT) ----------
| Statistics from Wed Jan 7 19:13:57 2004 to Wed Jan 7 19:14:00 2004
| Up since Mon Jan 5 21:44:37 2004 (1 day, 21:29)
| Last network change Mon Jan 5 21:44:36 2004
+----------
WatchGuard, Copyright (C) 1996-2003 WGTI
Firebox Release: andromeda
Driver version: 7.2.B1443
Daemon version: 7.2.B1443
Sys_B Version: 7.1.B1396
BIOS Version: fc82d0c4fce6d679245451c070eb511e Sicily
Serial Number: 408000056AB01
Product Type: Firebox X500
Product Options:

Packet counts

The number of packets allowed, denied, and rejected between status queries. Rejected packets are denied packets for which the Firebox sends an ICMP error message.

```
Allowed:        5832
Denied:         175
Rejects:        30
```

Log hosts

The IP addresses of the log host or hosts.

```
Log host(s):  206.148.32.16
```

Network configuration

Statistics about the network cards detected within the Firebox, including the interface name, its hardware and software addresses, and its netmask. In addition, the display includes local routing information and IP aliases.

```
Network Configuration:
lo local 127.0.0.1 network 127.0.0.0 netmask
255.0.0.0
eth0 local 192.168.49.4 network 192.168.49.0
netmask 255.255.255.0 outside (set)
eth1 local 192.168.253.1 network 192.168.253.0
netmask 255.255.255.0
```

Blocked Sites list

The current manually blocked sites, if any. Temporarily blocked site entries appear on the **Blocked Sites** tab.

```
Blocked list
network 10.0.0.0/8 permanent
network 172.16.0.0/12 permanent
network 192.168.0.0/16 permanent
```

Spoofing information

The IP addresses of blocked hosts and networks. If "none" is listed, the Firebox rejects these packets on all of its interfaces.

```
Spoofing info
Block Host 255.255.255.255 none
Block Network 0.0.0.0/8 none
Block Host 123.152.24.17 none
```

Logging options

Logging options configured with either the QuickSetup Wizard or by adding and configuring services from Policy Manager.

```
Logging options
Outgoing traceroute
Incoming traceroute logged(warning)
notifies(traceroute) hostile
Outgoing ping
Incoming ping
```

Authentication host information

The types of authentication being used and the IP address of the authentication server.

```
Authentication
Using local authentication for Remote User VPN.
Using radius authentication from
103.123.94.22:1645.
```

Memory

Statistics on the memory usage of the currently running Firebox. Numbers shown are bytes of memory.

```
Memory:
        total:    used:    free:  shared:
buffers: cached:
Mem:  65032192 25477120 39555072  9383936
9703424 362905
```

Load average

The number of jobs in the run queue averaged over 1, 5, and 15 minutes. The fourth number pair is the number of active processes per number of total processes running, and the last number is the next process ID number.

```
Load Average:
0.04 0.06 0.09 2/21 6282
```

Processes

The process ID, the name of the process, and the status of the process, as shown in the figure on the next page. (These codes appear under the column marked “S.”)

- R – Running
- S – Sleeping
- Z – Zombie

The other fields are as follows:

- RSS – Actual amount of RAM the process is using.
- SHARE – Amount of memory that can be shared by more than one process.
- TIME – Total CPU time used.
- (CPU) – Percentage of CPU time used.
- PRI – Priority of process.
- (SCHED) – The way the process is scheduled.

```
PID NAME                   S   RSS SHARE       TIME
(CPU) PRI (SCHED)
    1 init                   S  1136   564
148:41.84 ( 0)  99 (round robin)
    2 kflushd              S     0     0     0:00.02
( 0)   0 (nice)
```

```
    3 kswapd               S     0     0     0:00.00
( 0)   0 (fifo)
   55 nvstd                S   800   412     1:27.76
( 0)  98 (round robin)
   92 dvcpsv                  S  1284   628
3:33.43 ( 0)   2 (round robin)
 4287 iked                    S  1364   744
3:08.55 ( 0)   3 (round robin)
   71 fbr_mapper              S   256   176
0:00.16 ( 0)  98 (round robin)
   75 sslsrvd                 S  1648   976
0:00.37 ( 0)   0 (nice)
   73 fblightd                S   464   308
3927:05.75 ( 5)   0 (nice)
   74 /bin/logger             S  1372   592
1:29.72 ( 0)  99 (round robin)
   94 ppp-ttyS2               S   804   456
0:00.74 ( 0)   0 (nice)
   78 firewalld               R  2076  1248
307:29.75 ( 0)  98 (round robin)
   79 liedentd                S   708   356
0:00.03 ( 0)   0 (nice)
   80 dvcpd                   S  1152   576
57:00.26 ( 0)   0 (nice)
   82 fwcheck                 S   860   408
0:01.82 ( 0)  99 (round robin)
   95 /opt/bin/rbcast         S   784   372
0:39.47 ( 0)   3 (round robin)
   86 authentication          S  1112   496
0:02.21 ( 0)   3 (round robin)
   90 pswatch                 S   904   376
0:00.10 ( 0)   0 (nice)
   91 netdbg                  S   828   372
0:00.05 ( 0)   0 (nice)
   96 /opt/bin/dns-proxy      S   800   400
0:00.72 ( 0)   0 (nice)
```

Interfaces

Each network interface is displayed in this section, along with detailed information regarding its status and packet count. If you have purchased the Firebox X 3-Port Upgrade, the aliases eth3, eth4, and eth5 are also added.

```
Interfaces:
 lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Bcast:127.255.255.255
Mask:255.0.0.0
         UP BROADCAST LOOPBACK RUNNING  MTU:3584
Metric:0
        RX packets:0 errors:0 dropped:0 overruns:0
frame:0
        TX packets:0 errors:0 dropped:0 overruns:0
carrier:0
         Collisions:0
 eth0    Link encap:Ethernet  HWaddr
00:90:7F:1E:79:84
         inet addr:192.168.49.4
Bcast:192.168.49.255  Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
        RX packets:3254358 errors:0 dropped:0 over-
runs:0 frame:0
        TX packets:1662288 errors:0 dropped:0 over-
runs:0 carrier:0
         Collisions:193
             Interrupt:11 Base address:0xf000
 eth0:0  Link encap:Ethernet  HWaddr
00:90:7F:1E:79:84
         inet addr:192.168.49.5
Bcast:192.168.49.255  Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:1
        RX packets:3254358 errors:0 dropped:0 over-
runs:0 frame:0
        TX packets:1662288 errors:0 dropped:0 over-
runs:0 carrier:0
         Collisions:193
 eth1    Link encap:Ethernet  HWaddr
00:90:7F:1E:79:85
         inet addr:192.168.253.1
Bcast:192.168.253.255  Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500
Metric:2
        RX packets:6305057 errors:0 dropped:0 over-
runs:0 frame:0
```

```
        TX packets:7091295 errors:0 dropped:0 over-
runs:0 carrier:0
         Collisions:0
         Interrupt:10 Base address:0xec00
 ipsec0  Link encap:UNSPEC  HWaddr 00-90-7F-1E-79-
84-00-10-00-00-00-00-00-00-00-00
         inet addr:192.168.49.4
Bcast:192.168.49.255  Mask:255.255.255.0
         UP BROADCAST RUNNING NOARP MULTICAST
MTU:1400  Metric:5
        RX packets:0 errors:0 dropped:0 overruns:0
frame:0
        TX packets:0 errors:0 dropped:0 overruns:0
carrier:0
         Collisions:0
```

Routes

The Firebox kernel routing table. These routes are used to determine which interface the Firebox uses for each destination address.

```
Routes
Kernel IP routing table
Destination     Gateway       Genmask
Flags MSS    Window Use Iface
207.54.9.16     *           255.255.255.240 U
1500   0       58 eth0
207.54.9.48     *           255.255.255.240 U
1500   0       19 eth1
198.148.32.0    *           255.255.255.0   U
1500   0      129 eth1:0
127.0.0.0       *           255.0.0.0       U
3584   0        9 lo
default        207.54.9.30   *             UG
1500   0       95 eth0
```

ARP table

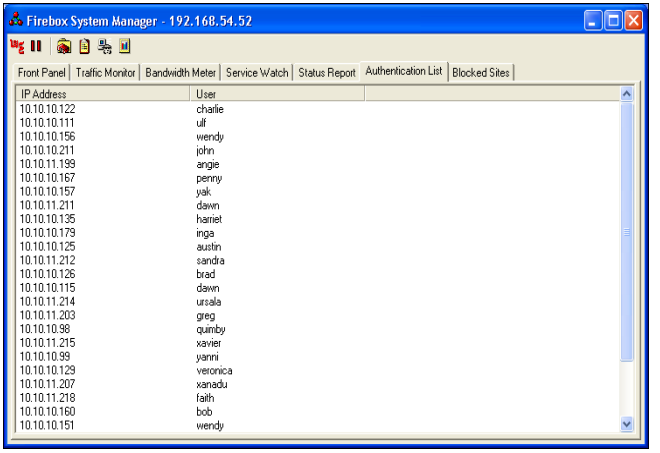
A snapshot of the ARP table on the running Firebox. The ARP table is used to map IP addresses to hardware addresses.

```
ARP Table
Address            HWtype  HWaddress
Flags Mask       Iface
207.23.8.32      ether   00:20:AF:B6:FA:29  C
*          eth1
207.23.8.52      ether   00:A0:24:2B:C3:E6  C
*          eth1
207.23.8.21      ether   00:80:AD:19:1F:80  C
*          eth0
201.148.32.54    ether   00:A0:24:4B:95:67  C
*          eth1:0
201.148.32.26    ether   00:A0:24:4B:98:7F  C
*          eth1:0
207.23.8.30      ether   00:A0:24:79:96:42  C
*          eth0
```

For more information on the status report page, see the following FAQ:
https://www.watchguard.com/support/advancedfaqs/log_statusall.asp

Authentication list

The **Authentication List** tab displays the host IP addresses and user names of everyone currently authenticated to the Firebox. If you are using DHCP, the IP address–to–user name mapping may change whenever machines restart.



Blocked Site list

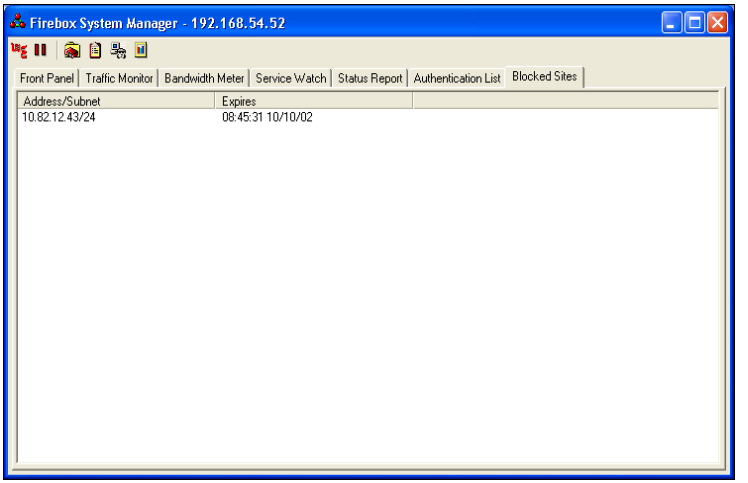
The **Blocked Site List** tab lists the IP addresses (in slash notation) of any external sites that are temporarily blocked by port space probes, spoofing attempts, address space probes, or another event configured to trigger an auto-block.

Next to each blocked site is the expiration time on the temporary auto-block. You can adjust the auto-blocking value from the **Blocked Sites** dialog box available through Policy Manager.

To remove a site from this list, right-click it and select **Remove Blocked Site**. If the display is in continuous refresh mode (that is, if the **Continue** button—shown at right—on the toolbar is active), selecting a site on the list stops the refresh mode.



If you opened the Firebox with the status (read-only) passphrase, System Manager prompts you to enter the configuration (read/write) passphrase before removing a site from the list.



HostWatch

HostWatch is a real-time display of active connections occurring on a Firebox. It can also graphically represent the connections listed in a log file, either playing back a previous file for review or displaying connections as they are logged into the current log file. HostWatch provides graphical feedback on network connections between the trusted and external networks as well as detailed information about users, connections, and network address translation.

The HostWatch display uses the logging settings configured with Policy Manager. For instance, to see all denied incoming Telnet attempts in HostWatch, configure the Firebox to log incoming denied Telnet attempts.

The line connecting the source host and destination host is color-coded to display the type of connection being made. These colors can be changed. The defaults are:

- **Red** – The connection is being denied.
- **Blue** – The connection is being proxied.
- **Green** – The connection is using network address translation (NAT).

- **Black** — The connection falls into none of the first three categories.

Representative icons appear next to the server entries for HTTP, Telnet, SMTP, and FTP.

Name resolution might not occur immediately when you first start HostWatch. As names are resolved, HostWatch replaces IP addresses with host or usernames, depending on the display settings. Some machines might never resolve and the IP addresses remain in the HostWatch window.

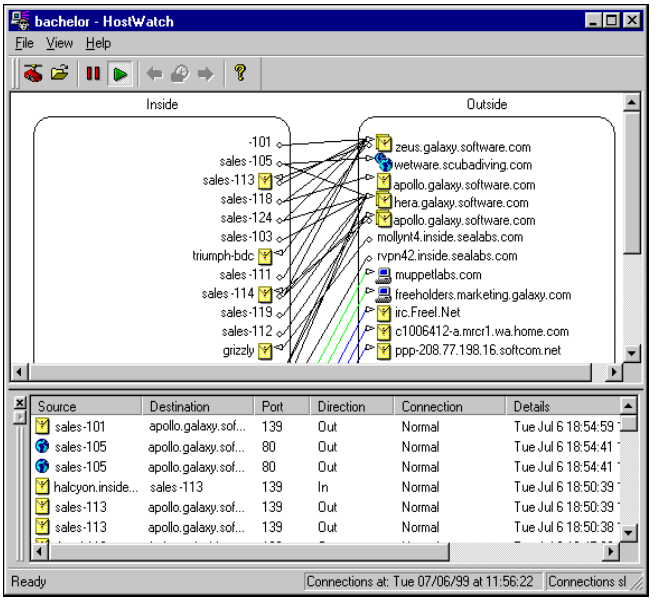


To start HostWatch, click the HostWatch icon (shown at left) on the Firebox System Manager.

HostWatch display

As shown in the following figure, the upper pane of the HostWatch display is split into two sides, Inside and Outside. Double-click an item on either side to produce a pop-up window displaying detailed information about current connections for the item, such as IP addresses, port number, connection type, and direction.

The lower pane displays the same information in tabular form, in addition to ports and the time the connection was established.



Connecting HostWatch to a Firebox

From HostWatch:

1 Select **File ⇒ Connect**.

Or, on the Hostwatch toolbar, click the Connect icon (shown at right).



2 Use the **Firebox** drop-down list to select a Firebox.

You can also type the Firebox name or IP address.

3 Enter the Firebox status passphrase. Click **OK**.

Replaying a log file in HostWatch

You can replay a log file in HostWatch in order to troubleshoot and retrace a suspected break-in. From HostWatch:

1 Select **File ⇒ Open**.

Browse to locate and select the log file. By default, log files are stored in the WatchGuard installation directory at C:\Program Files\WatchGuard\logs with the extension .wgl. HostWatch loads the log file and begins to replay the activity.



2 To pause the display, click Pause (shown at upper right).

3 To restart the display, click Continue (shown at right).



4 To step through the display one entry at a time, click the Pause icon. Click the right arrow to step forward through the log. Click the left arrow to step backward through the log.

Controlling the HostWatch display

You can selectively control the HostWatch display. This feature can be useful for monitoring the activities of specific hosts, ports, or users. From HostWatch:

1 Select **View ⇒ Filters**.

2 According to what you want to monitor, click the **Inside Hosts**, **Outside Hosts, Ports**, or **Authenticated Users** tab.

3 Clear the checkbox marked **Display All Hosts**, **Display All Ports**, or **Display All Authenticated Users**.

4 Enter the IP address, port number, or user ID you want to monitor. Click **Add**.
Repeat for each entity that HostWatch should monitor.

5 Click **OK**.

Modifying HostWatch view properties

You can change how HostWatch displays information. For example, HostWatch can display host names rather than IP addresses. From HostWatch:

1 Select **View ⇒ Properties**.

2 Use the **Host Display** tab to modify host display and text options.
For a description of each control, right-click it and then select What's This?.

3 Use the **Line Color** tab to choose colors for lines drawn between denied, dynamic NAT, proxy, and normal connections.

4 Use the **Misc.** tab to control the refresh rate of the real-time display and the maximum number of connections displayed.

CHAPTER 7

Configuring Network Address Translation

Network address translation (NAT) protects your network by hiding its internal structure. It also provides an effective way to conserve public IP addresses when the number of addresses is limited.

At its most basic level, NAT translates the address of a packet from one value to another. The "type" of NAT performed refers to the method of translation:

Dynamic NAT
Also called IP masquerading or port address translation. The Firebox either globally, or on a service-by-service basis, applies its public IP address to outgoing packets instead of using the IP address of the session behind the Firebox.

Static NAT
Also called port forwarding. Static NAT works on a port-to-host basis. Incoming packets from the external network destined for a specific public address and port are remapped to an address and port behind the firewall. You must configure each service separately for static NAT. Typically, static NAT is used for public services that do not require authentication such as Web sites and email.

1-to-1 NAT
The Firebox uses private and public IP ranges that you specify, rather than the ranges assigned to the Firebox interfaces during configuration.

Choosing which type of NAT to perform depends on the underlying problem being solved, such as those regarding address security or preservation of public IP addresses. For more information on NAT, see the following collection of FAQs: https://www.watchguard.com/support/advancedfaqs/nat_main.asp

Dynamic NAT

Dynamic NAT is the most commonly used form of NAT. It works by translating the source IP address of outbound sessions (those originating on the internal side of the Firebox) to the one public IP address of the Firebox. Hosts elsewhere see only outgoing packets from the Firebox itself.

This type of NAT is most commonly used to conserve IP addresses. It allows multiple computers to access the Internet by sharing one public IP address. Even if the number of public IP addresses is not a concern, dynamic NAT provides extra security for internal hosts that use the Internet by allowing them to use non-routable addresses.

WatchGuard System Manager implements two forms of outgoing dynamic NAT:

Simple dynamic NAT
Using host aliases or host and network IP addresses, the Firebox globally applies network address translation to every outgoing packet. This is the most commonly used type of NAT.

Service-based dynamic NAT
Each service is configured individually for outgoing dynamic NAT. This type of NAT is generally used only in conjunction with drop-in mode.

NOTE

Machines making incoming requests over a VPN connection are allowed to access masqueraded hosts by their actual private addresses.

Using Simple Dynamic NAT

In the majority of networks, the preferred security policy is to globally apply network address translation to all outgoing packets. Simple dynamic NAT provides a quick method to set a NAT policy for your entire network. For more information on this type of NAT, see the following FAQ:
https://www.watchguard.com/support/advancedfaqs/nat_howdynamicnat.asp

Enabling simple dynamic NAT

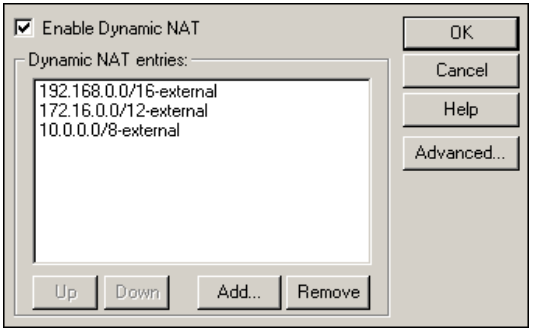
The default configuration of simple dynamic NAT enables it from all non-routable addresses to the external network. From Policy Manager:

1 Select **Setup ⇒ NAT**.
The NAT Setup dialog box appears, as shown in the following figure.

2 Select the checkbox marked **Enable Dynamic NAT**.

The default dynamic entries are:

- 192.168.0.0/16 - external
- 172.16.0.0/12 - external
- 10.0.0.0/8 - external
  These are the private networks defined by RFC. If you are using public IP addresses other than these, you must add an entry (unless you're using drop-in mode).



Adding simple dynamic NAT entries

Using built-in host aliases, you can quickly configure the Firebox to masquerade addresses from your trusted and optional networks. If trusted hosts are already covered by the default, non-routable ranges, no additional entries are needed:

- From: Trusted
- To: External

The default dynamic entries are listed in the previous section.

Larger or more sophisticated networks may require additional entries in the **From** or **To** lists of hosts or host aliases. The Firebox applies dynamic NAT rules in the order in which they appear in the Dynamic NAT Entries list. WatchGuard recommends prioritizing entries based on the volume of traffic that each represents. From the **NAT Setup** dialog box:

1 Click **Add**.

2 Use the **From** drop-down list to select the origin of the outgoing packets.

For example, use the trusted host alias to globally enable network address translation from the trusted network. For a definition of built-in Firebox aliases, see "Using Aliases" on page 150. For more information on how to add a user-defined host alias, see "Adding an alias" on page 151.

3 Use the **To** drop-down list to select the destination of outgoing packets.

4 To add either a host or network IP address, click the **...** button. Use the drop-down list to select the address type.

Enter the IP address or range. Network addresses must be entered in slash notation.

When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For information on entering IP addresses, see "Entering IP addresses" on page 37.

5 Click **OK**.

The new entry appears in the Dynamic NAT Entries list.

Reordering simple dynamic NAT entries

To reorder dynamic NAT entries, select the entry and click either **Up** or **Down**. There is no method to modify a dynamic NAT entry. Instead, use the **Remove** button to remove existing entries and the **Add** button to add new entries.

Specifying simple dynamic NAT exceptions

You can set up ranges of addresses in dynamic NAT so that each address in that range is a part of the NAT policy. By using the dynamic NAT exceptions option you can exclude certain addresses from that policy.

From Policy Manager:

1 Select **Setup** ⇒ **NAT**.

The NAT Setup dialog box appears.

2 Click **Advanced**.

The Advanced NAT Settings dialog box appears.

3 Click the **Dynamic NAT Exceptions** tab.

4 Click **Add**.

The Add Exception dialog box appears.

5 In the **From** and **To** boxes, select the appropriate interface.

The choices dvcp_nets and dvcp_local_nets are aliases for VPN Manager and appear if your Firebox is configured as a DVCP client. dvcp_nets refers to networks at the other end of the VPN tunnel and dvcp_local_nets refers to networks behind the Firebox being configured. Under normal circumstances, you should not make dynamic NAT exceptions for these networks.

6 Click the button next to the **From** box and enter the value of the host IP address, network IP address, or host range. Click **OK**.

7 Click **OK** to close the **Advanced NAT Settings** dialog box.

NOTE

Dynamic NAT exceptions allow the configuration of exceptions to both forms of dynamic NAT. You will need to make dynamic NAT exceptions for any 1-to-1 NAT address that would otherwise be subject to dynamic NAT.

Using Service-Based Dynamic NAT

Using service-based dynamic NAT, you can set outgoing dynamic NAT policy on a service-by-service basis. Service-based NAT is most frequently used to make exceptions to a globally applied simple dynamic NAT entry.

For example, use service-based NAT on a network with simple NAT enabled from the trusted to the optional network with a Web server on the optional network that should not be masqueraded to the actual trusted network. Add a service icon allowing Web access from the trusted to the optional Web server, and disable NAT. In this configuration, all Web access from the trusted network to the Web server is made with the true source IP, and all other traffic from trusted to optional is masqueraded.

You can also use service-based NAT instead of simple dynamic NAT. Rather than applying NAT rules globally to all outgoing packets, you can start from the premise that no masquerading takes place and then selectively masquerade a few individual services.

Enabling service-based dynamic NAT

Service-based NAT is not dependent on enabling simple dynamic NAT. From Policy Manager:

1 Select **Setup** ⇒ **NAT**. Click **Advanced**.

2 Select the checkbox marked **Enable Service-Based NAT**.

3 Click **OK** to close the **Advanced NAT Settings** dialog box. Click **OK** to close the **NAT Setup** dialog box.

Configuring service-based dynamic NAT

By default, services take on whatever dynamic NAT properties you have set for simple NAT. However, you can override this set-

ting in the service's **Properties** dialog box. You have three options:

Use Default (Simple NAT)
Service-based NAT is not enabled for the service. The service uses the simple dynamic NAT rules configured in the **Dynamic NAT Entries** list, as explained in "Adding simple dynamic NAT entries" on page 98.

Disable NAT
Disables dynamic NAT for outgoing packets using this service. Use this setting to create service-by-service exceptions to outgoing NAT.

Enable NAT
Enables service-based dynamic NAT for outgoing packets using this service regardless of how the simple dynamic NAT settings are configured.

From Policy Manager:

1 Double-click the service icon. Click **Outgoing**.

2 Use the **Choose Dynamic NAT Setup** drop-down list to select either the default (simple dynamic NAT), disable, or enable setting. Click **OK**.



Configuring Service-Based Static NAT

For more information on static NAT, see the following FAQs:
https://www.watchguard.com/support/advancedfaqs/nat_whenstatic.asp
https://www.watchguard.com/support/advancedfaqs/nat_outin.asp

Adding external IP addresses

Static NAT converts a Firebox public IP and port into specific destinations on the trusted or optional networks. If you want to use an address other than that of the external interface itself,

you must designate a new public IP address using the **Add External IP** dialog box. From Policy Manager:

1 Select **Network** ⇒ **Configuration**. Click the **Aliases** button.
The Add External IP dialog box appears.

2 At the bottom of the dialog box, enter the public IP address. Click **Add**.

3 Repeat until all external public IP addresses are added. Click **OK**.

Setting static NAT for a service

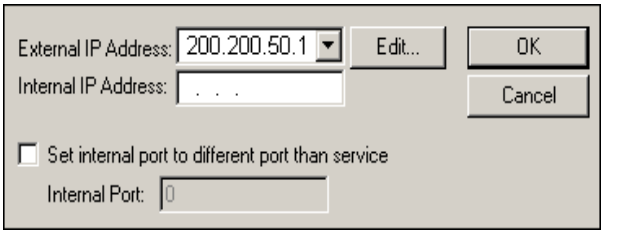
Static NAT, like service-based NAT, is configured on a service-by-service basis. Because of the way static NAT functions, it is available only for services based upon TCP or UDP, which use a specific port. A service containing any other protocol cannot use incoming static NAT, and the **NAT** button in the service's **Properties** dialog box is disabled. Static NAT also cannot be used with the Any service. See the following FAQ before configuring static NAT for a service:
https://www.watchguard.com/support/advancedfaqs/nat_outin.asp

1 Double-click the service icon in the Services Arena.
The service's Properties dialog box appears displaying the Incoming tab.

2 Use the **Incoming** drop-down list to select **Enabled and Allowed**.
To use static NAT, the service must allow incoming traffic.

3 Under the **To** list, click **Add**.
The Add Address dialog box appears.

4 Click **NAT**.
The Add Static NAT dialog box appears, as shown in the following figure.



NOTE

Mail servers should either use the actual external address of the Firebox for inbound NAT, or they should use 1-to-1 NAT. Otherwise, mail delivery problems could occur.

5 Use the **External IP Address** drop-down list to select the "public" address to be used for this service.
   If the public address does not appear in the drop-down list, click Edit to open the Add External IP dialog box and add the public address.

6 Enter the internal IP address.
   The internal IP address is the final destination on the trusted network.

7 If appropriate, select the checkbox marked **Set internal port to different port than service**.
   This feature is rarely required. It enables you to redirect packets not only to a specific internal host but also to an alternative port. If you select the checkbox, enter the alternative port number in the Internal Port field.

8 Click **OK** to close the **Add Static NAT** dialog box.
   The static NAT route appears in the Members and Addresses list.

9 Click **OK** to close the **Add Address** dialog box. Click **OK** to close the services's **Properties** dialog box.

Using 1-to-1 NAT

1-to-1 NAT uses a global NAT policy that rewrites and redirects packets sent to one range of addresses to a completely different range of addresses. This address conversion works in both directions. You can configure any number of 1-to-1 NAT addresses.

A common reason to use 1-to-1 NAT is to map public IP addresses to internal servers without needing to renumber those servers. 1-to-1 NAT is also used for VPNs in which the remote network's IP addressing scheme conflicts with the local scheme. By translating the local network to a range that is not in conflict with the other end, both sides can communicate. For more information on 1-to-1 NAT, see the following FAQ: https://www.watchguard.com/support/advancedfaqs/nat_onetoone.asp

Each NAT policy contains four configurable pieces of information:

- The interface
- The public IP address
- The internal IP address
- The number of hosts to remap

The NAT base plus the range defines the NAT region while the real base plus the range defines the hidden or forwarded region.

For instance, the following policy:

```
210.199.6.1-192.168.69.1:254 (NAT base to real base range)
```

means that all traffic addressed to hosts between 210.199.6.1 and 210.199.6.254 is forwarded to the corresponding IP address between 192.168.69.1 and 192.168.69.254.

A one-to-one mapping exists between each NAT address and the forwarded (real) IP address: 210.199.6.0 becomes 192.168.69.0.

From Policy Manager:

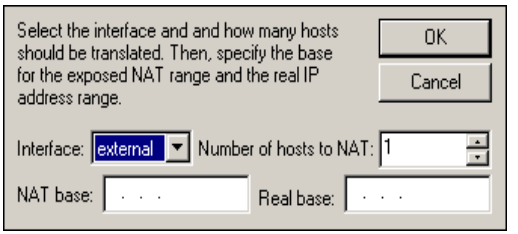
1 Select **Setup** ⇒ **NAT**.
The NAT Setup dialog box appears.

2 Click **Advanced**.
The Advanced NAT Settings dialog box appears.

3 Click the **1-to-1 NAT Setup** tab.

4 Select the checkbox marked **Enable 1-1 NAT**.

5 Click **Add**.
The 1-1 Mapping dialog box appears, as shown in the following figure.


Select the interface and and how many hosts should be translated. Then, specify the base for the exposed NAT range and the real IP address range.
OK
Cancel
Interface:
external
Number of hosts to NAT:
1
NAT base:
Real base:

6 Select the appropriate interface.

7 Enter the number of hosts to be translated.

8 In the **NAT base** field, enter the base address for the exposed NAT range.

This will generally be the public IP address that will appear outside the Firebox.

9 In the **Real base** field, enter the base address for the real IP address range. Click **OK**.

This will generally be the private IP address directly assigned to the server or client.

10 Click the **Dynamic NAT Exceptions** tab.

You must make dynamic NAT exceptions for any internal address being used for 1-to-1 NAT; otherwise, the address will be translated using dynamic NAT instead of 1-to-1 NAT.

11 Click **Add**.

The Add Exception dialog box appears.

12 In the **To** box, select the appropriate interface. In most cases, you will choose the external interface.

The choices dvcp_nets and dvcp_local_nets are aliases for VPN Manager and appear if your Firebox is configured as a DVCP client. dvcp_nets refers to networks at the other end of the VPN tunnel and dvcp_local_nets refers to networks behind the Firebox being configured. Under normal circumstances, you should not make dynamic NAT exceptions for these networks.

13 Click the button next to the **From** box and enter the value of the real IP address range, as entered in step 9. Click **OK**.

14 Click **OK** to close the **Advanced NAT Settings** dialog box. Click **OK** to close the **NAT Setup** dialog box.

Proxies and NAT

The table on the following page identifies each proxy and what types of NAT it supports.

	Simple dynamic	Static	Service-based	1-to-1
DNS	yes	yes	yes	yes
HTTP	yes	yes	yes	yes
SMTP	yes	yes	yes	yes
FTP	yes	yes	yes	yes
DCE-RPC	yes	no	no	no
H323	yes	no	no	no
RTSP	yes	yes	no	no
RealNetworks	no	no	no	no

CHAPTER 8

Configuring Filtered Services

You add filtered services—in addition to proxied services—to control and monitor the flow of IP packets through the Firebox. Services can be configured for outgoing and incoming traffic, and they can be active or inactive. When you configure a service, you set the allowable traffic end points and determine the filter rules and policies for each of these services. You can also create services to customize rule sets, destinations, protocols, ports used, and other parameters. With both packet filters and proxies, you can determine which hosts within your LAN and on the Internet can communicate with each other through that protocol, which events to log (such as rejected incoming packets), and which series of events should initiate a notification of the network administrator.

For information on the different types of services available, see Chapter 3, "Types of Services," in the *Reference Guide*. For information specifically on proxied services, see Chapter 9, "Configuring Proxied Services," in this manual. See also the Services FAQ on the WatchGuard Web site: https://www.watchguard.com/support/advancedfaqs/svc_main.asp

Selecting Services for your Security Policy Objectives

The WatchGuard System Manager, like most commercial firewalls, discards all packets that are not explicitly allowed, often stated as "that which is not explicitly allowed is denied."

This stance protects against attacks based on new, unfamiliar, or obscure IP services. It also provides a safety net regarding unknown services and configuration errors which could otherwise threaten network security. This also means that for the Firebox to pass *any* traffic, it must be configured to do so. You must actively select the services and protocols allowable, configure each one as to which hosts can send and receive them, and set other properties individual to the service.

Every service brings tradeoffs between network security and accessibility. When selecting services, balance the needs of your organization with the requirement that computer assets be protected from attack.

Incoming and outgoing services

For basic information on incoming and outgoing traffic and how it relates to the different Firebox interfaces, see "About Incoming and Outgoing Traffic" on page 67.

A connection from a less trusted segment to a more trusted segment is incoming and must be configured on the **Incoming** tab for the service, as described in "Defining Service Properties" on page 117. Likewise, a connection from a more trusted segment to a less trusted segment is outgoing and must be configured on the **Outgoing** tab for the service.

For example, suppose you wanted to allow Telnet connections from the eth5 network to the eth2 network. This would be configured on the **Incoming** tab for the Telnet service, because the direction of data flow is from a less trusted network to a more trusted network.

Or, suppose you wanted to allow HTTP connections from a VPN source that is using the Firebox as the default route back out to the external interface. In this instance, you would use the **Outgoing** tab for the HTTP service, because VPN sources are more trusted than external sources.

Incoming service guidelines

Enabling incoming services creates a conduit into your network. The following are some guidelines for assessing security risks as you add incoming services to a Firebox configuration:

- A network is only as secure as the least secure service allowed into it.
- Services you do not understand should not be trusted.
- Services with no built-in authentication and those not designed for use on the Internet are risky.
- Services that send passwords in the clear (FTP, telnet, POP) are very risky.
- Services with built-in strong authentication (such as ssh) are reasonably safe. If the service does not have built-in authentication, you can mitigate the risk by using user authentication with that service.
- Services such as DNS, SMTP, anonymous FTP, and HTTP are safe only if they are used in their intended manner.
- Allowing a service to access only a single internal host is safer than allowing the service to access several or all hosts.
- Allowing a service from a restricted set of hosts is somewhat safer than allowing the service from anywhere.
- Allowing a service to the optional network is safer than allowing it to the trusted network.
- Allowing incoming services from a virtual private network (VPN), where the organization at the other end is known and authenticated, is generally safer than allowing incoming services from the Internet at large.

Each safety precaution you implement makes your network significantly safer. Following three or four precautions is much safer than following one or none.

Outgoing service guidelines

In general, the greatest risks come from incoming services, not outgoing services. There are, however, some security risks with outgoing services as well. Control of outgoing services helps to protect your network from hostile acts within your organization. For example, when configuring the outgoing FTP service, you

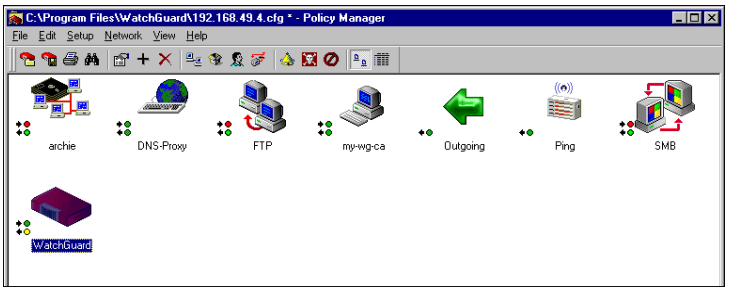
can make it read-only and/or restrict the destination hosts that can receive such a transmission. This prevents insiders from using FTP to transmit corporate secrets to a home computer or to a rival organization.

As another example, passwords used for some services (FTP, telnet, POP) are sent in the clear. If the passwords are the same as those used internally, a hacker can hijack that password and use it to gain access to your network.

Adding and Configuring Services

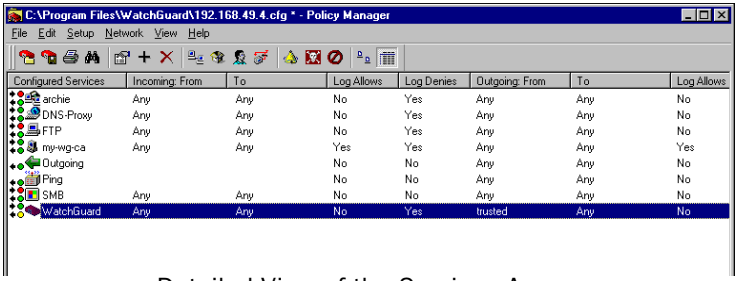
You add and configure services using Policy Manager. The Services Arena of Policy Manager contains icons that represent the services (filtered and proxied) currently configured on the Firebox, as shown in the following figure. You can choose from many filtered and proxied services. These services are configurable for outgoing or incoming traffic, and they can also be made active or inactive. When configuring a service, you set the allowable traffic sources and destinations, as well as determine the filter rules and policies for the service. You can create services to customize rule sets, destinations, protocols, ports used, and other parameters.

You can also add unique or custom services. However, if you do, take steps to permit only the traffic flow in that service that is absolutely essential.



Normal View of the Services Arena

To display the detailed view of the Services Arena, select the Details icon (shown at right) at the far right of the toolbar. The detailed view appears, as shown in the following figure.


C:\Program Files\WatchGuard\192.168.49.4.cfg * - Policy Manager
File Edit Setup Network View Help
Configured Services | Incoming: From | To | Log Allows | Log Denies | Outgoing: From | To | Log Allows
archie | Any | Any | No | Yes | Any | Any | No
DNS-Proxy | Any | Any | No | Yes | Any | Any | No
FTP | Any | Any | No | Yes | Any | Any | No
my-wg-ca | Any | Any | Yes | Yes | Any | Any | Yes
Outgoing | | | No | No | Any | Any | No
Ping | | | No | No | Any | Any | No
SMB | Any | Any | No | No | Any | Any | No
WatchGuard | Any | Any | No | Yes | trusted | Any | No

Detailed View of the Services Arena

To return to the normal view of the Services Arena, select the Large Icons button (shown at right).

Configurable parameters for services

Several service parameters can be configured:

Sources and Destinations

You use separate controls for configuring incoming and outgoing traffic. The outgoing controls (sources) define entries in the **From** lists while incoming controls (destinations) define entries in the **To** lists.

Logging and Notification

Each service has controls that enable you to select which events for that service are logged, and whether you want to be notified of these events.

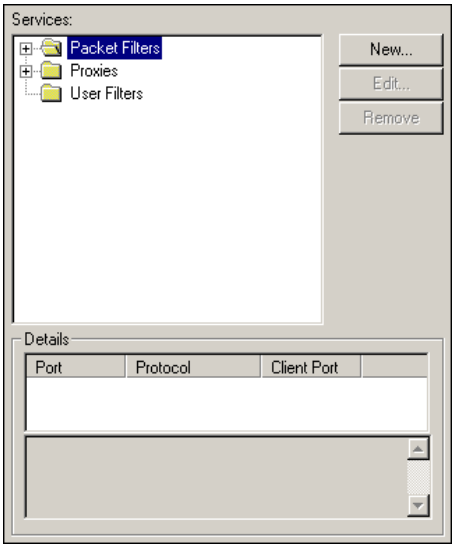
Adding a service

You use Policy Manager to add existing, preconfigured filtering and proxied services to your configuration file.

To add a new service to your firewall policy:

1 On the Policy Manager toolbar, click the Add Services icon (shown at right).

You can also select, from the menu bar, Edit ⇒Add Service. The Services dialog box appears, as shown in the following figure. You use this dialog box to add, modify, and remove the filtered and proxed services you want.



2 Expand either the **Packet Filters** or **Proxies** folder by clicking the plus (+) sign to the left of the folder.
A list of pre-configured filters or proxies appears.

3 Click the name of the service you want to add.
When you click a service, the service icon appears in the area below the New, Edit, and Remove buttons. Also, the Details box displays basic information about the service.

4 Click **Add**.
The Add Service dialog box appears, as shown in the following figure.



5 (Optional) You can customize both the name and the comments that appear when the service is being configured.

Click in the **Name** or **Comment** box and type the name or comment you want.

6 Click **OK**.

The service's Properties dialog box appears. For information on configuring service properties see, "Defining Service Properties" on page 117.

7 Click **OK** to close the **Properties** dialog box.

You can add more than one service while the Services dialog box is open.

8 Click **Close**.

The new service appears in Policy Manager Services Arena.

Adding multiple services of the same type

In developing a security policy for your network, you might want to add the same service more than once. For example, you might need to restrict Web access for the majority of your users while allowing complete Web access to your executive team. To do this, you would create two separate HTTP services with different properties for the outgoing rule.

1 Add the first service, as described in steps 1 – 4 in "Adding a service" on page 111.

2 Modify the name of the service to reflect its role within your security policy and add any relevent comments.

Using the example of separate HTTP services described previously, you might call the first HTTP service "restricted_web_access."

3 Click **OK** to bring up the service's **Properties** dialog box and define outgoing properties, as described in "Adding service properties" on page 118.

Using the previous example, you might add an alias called "staff," which includes a range of IP addresses or group of authenticated users. For more information on aliases, see "Using Aliases" on page 150.

4 Add the second HTTP service.

Using the previous example, you might call this second HTTP service "full_web_access."

5 Click **OK** to bring up the service's **Properties** dialog box and define outgoing properties, as described in "Adding service properties" on page 118.

Using the previous example, you might add an alias called "executives."

NOTE

Be careful to avoid creating conflicting services; for example, one HTTP service that allows incoming traffic while the other is set to deny incoming traffic. You can use the Disabled option to allow multiple services without conflicts.

Creating a new service

In addition to built-in filtered services provided by WatchGuard, you can create a new service or customize an existing service. You might need to do this when a new product appears on the market that you would like to run behind your firewall. Remember, however, that every new service you configure and add to your firewall potentially increases your vulnerability to hackers.

From Policy Manager:

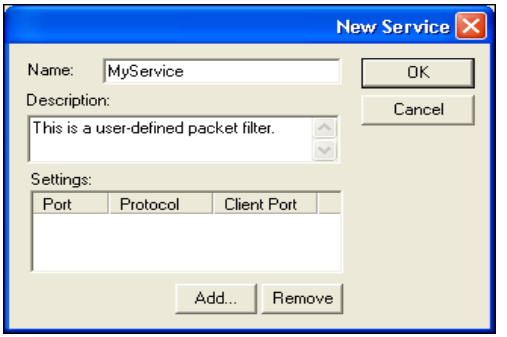
1 On the Policy Manager toolbar, click the Add Services icon (shown at right).



The Services dialog box appears.

2 Click **New.**

The New Service dialog box appears, as shown in the following figure.



3 In the **Name** text box, type the name of the service.

This name must be unique and not already listed in the Services dialog box.

4 In the **Description** text box, type a description of the service.

This description appears in the Details section of the New Services dialog box when you select the service.

5 To begin setting the port used for this service, click **Add.**

The Add Port dialog box appears.

6 From the **Protocol** drop-down list, select the protocol used for this new service. The following options are available:

TCP
TCP-based services

UDP
UDP-based services

HTTP
Services examined by the HTTP proxy

IP
Filter a service using something other than TCP (IP protocol 6) or UDP (IP protocol 17) for the next-level protocol. Select **IP** to create a protocol number service.

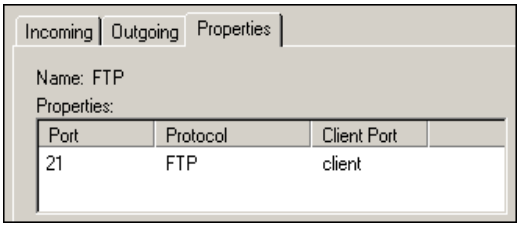
7 In the **Client Port** text box, select an option from the drop-down list. Note that you can select a range of port numbers. The following options are available:

Ignore
Source port can be any number (0–65565). (If you are not sure which port setting to use, choose this option.)

Secure
Source port can range from 0–1024.

Port
Source port must be identical to the destination port, as listed in the **Port** number field of the destination service's **Properties** dialog box, **Properties** tab (shown below).

Client
Source port can range from 1025–65565.



8 In the **Port** field, enter the port number. If you are entering a range, enter the lowest number of the range.

9 In the **To** field, enter the highest number of the range. (If you are not entering a range, leave this field blank.)

10 Click **OK**.

Policy Manager adds the port configuration to the New Service dialog box. An example of how this dialog box might look appears in the following figure. Verify that the name, description, and configuration of this service are correct. If necessary, click Add to configure an additional port for this service. Repeat the process until all ports for the service are configured.



11 Click **OK**.

The Services dialog box appears with the new service displayed under the User Filters folder. You can now add the custom service to the Services Arena just as you would an existing service.

12 In the **Services** dialog box, expand the **User Filter** folder, and then click the name of the service. Click **Add** and then click **OK** to close the **Add Service** dialog box. Click **OK** to close the **Properties** dialog box. Click **Close** to close the **Services** dialog box.

The icon of the new service appears in the Services Arena.

Deleting a service

From Policy Manager:

1 In the Services Arena, click the icon of the service you want to delete.

2 On the toolbar, click the Delete Service icon (shown at right).



You can also select Edit ⇒Delete or right-click the icon and select Delete.

3 When asked to confirm, click **Yes**.
The service is removed from the Services Arena.

4 Save the configuration to the Firebox and reboot the Firebox. To do this, select **File ⇒Save ⇒To Firebox**. Enter the configuration passphrase when prompted. In the dialog box that appears, select the **Save to Firebox** checkbox.

Defining Service Properties

You use the service's **Properties** dialog box to configure the incoming and outgoing access rules for a given service.

The **Incoming** tab defines:

- The sources on the external network (or a less trusted network) that use this service to initiate sessions with your protected users, hosts, and networks.
- The destinations behind the Firebox to which incoming traffic for this service can be bound.

The **Outgoing** tab defines:

- The sources behind the Firebox that use this service to initiate sessions with an outside (or less trusted) destination.
- The destinations on the external network to which outgoing traffic for this service can be bound.

In a given direction, a service can be in one of three states:

Disabled
The traffic is handled by any other rules that might apply to it. If none exists, the packets are denied by default packet handling and logged as such. You can make any service a one-directional filter by selecting **Disabled** on either the **Incoming** or **Outgoing** tab. This is generally used when configuring multiple policies for the same service, such as HTTP.

Enabled and Denied
No traffic is allowed through this service, and packets for this service will be blocked. The service logs the attempts to connect to it.

Enabled and Allowed
Traffic is allowed through this service in the selected direction according to the From and To properties.

Accessing a service's Properties dialog box

When you add a service, the service's **Properties** dialog box automatically appears. You can bring up an existing service's **Properties** dialog box either by double-clicking the service icon in the Services Arena or by selecting the services icon and clicking the Edit Service icon (shown at right).



Adding service properties

The method used to add incoming and outgoing service properties is identical. Select the tab, click the **Add** button for either the From or the To member list, and then define the members for the category. The direction of traffic determines how you select members of the From and To lists.

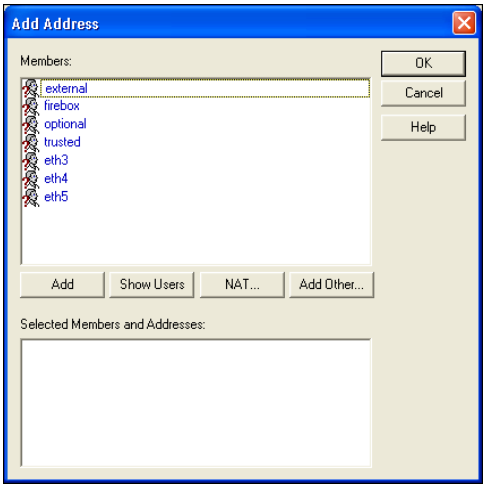
Tab	Member List	Defines
Incoming	From	External users or hosts that the service will allow in
Incoming	To	Destinations within the trusted network that can receive packets through the service
Outgoing	From	Users and hosts on the trusted network that can send packets out through the service
Outgoing	To	Destinations on the external network to which traffic for this service can be found

Adding addresses or users to service properties

Both the Incoming and Outgoing properties include From and To address lists. Use the **Add Address** dialog box to add a network, IP address, or specific user to a given service.

1 In the **Properties** dialog box, use the **Incoming service Connections Are** drop-down list to select **Enabled and Allowed**.

2 Click either the **Incoming** tab or **Outgoing** tab. Click the **Add** button underneath the **From** or the **To** list.
The Add Address dialog box appears, as shown in the following figure.



3 Click **Add Other**.
The Add Member dialog box appears.

4 From the **Choose Type** drop-down list, click the type of address, range, host name, or user you want to add.

5 In the **Value** text box, type the actual address, range, or name. Click **OK**.
The member or address appears in the Selected Members and Addresses list.

6 Click **OK**.
The new selection appears in either the Incoming or Outgoing tab under the appropriate From or To box.

Working with wg_icons

Service icons beginning with "wg_" are created automatically when you enable features such as PPTP and authentication. Because the wg_ service icons rarely require modification, WatchGuard recommends leaving wg_ icons in their default settings.

The following wg_ services are available:

wg_authentication
Added when you enable authentication.

wg_dhcp_server
Added when you enable the DHCP server.

wg_pptp
Added when you enable PPTP.

wg_dvcp
Added when the device has been inserted into VPN Manager.

wg_sohomgt
Added when you enable the DVCP server.

wg_ca
Added when you enable the DVCP server, which also configures the Firebox as a certificate authority.

The wg_ icons appear in the Services Arena when you select **View ⇒ Hidden Services** such that a checkmark appears next to the menu option. To hide the wg_ icons, select **View ⇒ Hidden Services** again such that the checkmark disappears.

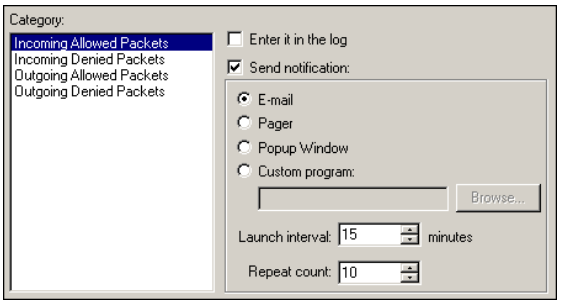
Customizing logging and notification

WatchGuard System Manager allows you to create custom logging and notification properties for each filtered service, proxied service, and blocking option. This level of flexibility allows you to fine-tune your security policies, logging only those events that require your attention and limiting notification to truly high-priority events.

You use the **Logging and Notification** dialog box to configure the services, blocking categories, and packet handling options you want. Consequently, once you master the controls for one type of service, the remainder are easy to configure.

1 From the **Properties** dialog box, click the **Incoming** tab. Click **Logging**.
The Logging and Notification dialog box appears.

2 Enable the options you want, as described below.



The **Logging and Notification** dialog box contains the following controls:

Category
The list of event types that can be logged by the service or option. This list changes depending on the service or option you've selected. You click the event name to display and set its properties.

Enter it in the log
When you select this checkbox, an entry appears in the log file each time someone on the external network uses the service incorrectly. For example, if someone attempts to send a packet to an address other than the host IP address you specified when defining service properties, the packet is denied and an entry made in the log file.

Send notification
When you select this checkbox, a notification is sent every time packets are denied. You set notification criteria using the WatchGuard Security Event Processor (WSEP). For more information, see "Customizing Logging and Notification by Service or Option" on page 197.

The remaining controls are active when you select the **Send notification** checkbox:

Email
Triggers an email message when the event occurs. Set the email recipient in the **Notification** tab of the WatchGuard Security Event Processor (WSEP) user interface.

Pager
Triggers an electronic page when the event occurs. The Firebox must have a PCMCIA modem and be connected to a phone service to make outgoing calls. (If the pager is accessible by email, you can enable notification by email and then enter the email address of the pager in the appropriate field.)

Popup window
Brings up a window when the event occurs.

Custom program
Runs a program when the event occurs. Enter the path of the executable file in the box provided, or browse to specify a path.

Launch interval and repeat count work in conjunction to control notification timing. For more information on this setting, see "Setting Launch Interval and Repeat Count" on page 199.

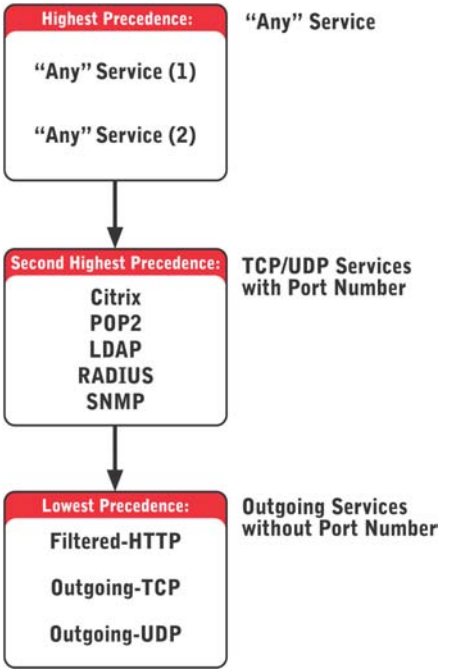
Service Precedence

Precedence is generally given to the most specific service and descends to the most general service. However, exceptions exist. There are three different precedence groups for services:

- The "Any" service (see the *Reference Guide* for more information about the "Any" filtered service). This group has the highest precedence.
- IP and ICMP services and all TCP/UDP services that have a port number specified. This group has the second highest precedence and is the largest of the three.
- "Outgoing" services that do not specify a port number (they apply to any port). This group includes Outgoing TCP, Outgoing UDP, and Proxy.

"Multiservices" can contain subservices of more than one precedence group. "Filtered-HTTP" and "Proxied-HTTP," for example, contain both a port-specific TCP subservice for port 80 as well as a nonport subservice that covers all other TCP connections. When precedence is being determined, individual subservices are given precedence according to their group (described previously) independent of the other subservices contained in the multiservice.

Precedence is determined by group first. As shown in the following diagram, services from a higher precedence group always have higher precedence than the services of a lower precedence group, regardless of their individual settings. For example, because the "Any" service is in the highest precedence group, all incidences of the "Any" service will take precedence over the highest precedence Telnet service.



The precedences of services that are in the same precedence group are ordered from the most specific services (based on source and destination targets) to the least specific service. The method used to sort services is based on the specificity of targets, from most specific to least specific.

The following order is used:

From	To	Rank
IP	IP	0
List	IP	1
IP	List	2
List	List	3
Any	IP	4
IP	Any	5
Any	List	6

From	To	Rank
List	Any	7
Any	Any	8

IP refers to exactly one host IP address
List refers to multiple host IP addresses, a network address, or an alias
Any refers to the special "Any" target (not "Any" services)

When two icons are representing the same service (for example, two Telnet icons or two Any icons), they are sorted using the above tables. The most specific one will always be checked first for a match. If a match is not made, the next specific service will be checked, and so on, until either a match is made or no services are left to check. In the latter case, the packet is denied. For example, if there are two Telnet icons, telnet_1 allowing from A to B and telnet_2 allowing from C to D, a Telnet attempt from C to E will first check telnet_1, and then telnet_2. Because no match is found, the rest of the rules are considered. If an outgoing service allows from C to E, it will do so.

When only one icon is representing a service in a precedence category, only that service is checked for a match. If the packet matches the service and both targets, the service rule applies. If the packet matches the service but fails to match either target, the packet is denied. For example, if one Telnet icon allows from A to B, a Telnet attempt from A to C will be blocked without considering any services further down the precedence chain, including outgoing services.

For more information on outgoing services, see the following FAQ:
https://www.watchguard.com/support/advancedfaqs/svc_outgoing.asp

CHAPTER 9

Configuring Proxied Services

Proxy filtering goes a step beyond packet filtering by examining a packet's content, not just the packet's header. Consequently, the proxy determines whether a forbidden content type is hidden or embedded in the data payload. For example, an email proxy examines all SMTP packets to determine whether they contain forbidden content types, such as executable programs or items written in scripting languages. Such items are common methods of transmitting computer viruses. The SMTP proxy knows these content types are not allowed, while a packet filter would not detect the unauthorized content in the packet's data payload.

Proxies work at the application level, while packet filters work at the network and transport protocol level. In other words, each packet processed by a proxy is stripped of all network wrapping, analyzed, rewrapped, and forwarded to the intended destination. This adds several layers of complexity and processing beyond the packet filtering process. What this means, of course, is that proxies use more processing bandwidth than packet filters. On the other hand, they catch dangerous content types in ways that packet filters cannot.

To add or configure a proxied service, use the procedures for filtered services in the previous chapter, "Configuring Filtered

Services." For more information on proxies, see the following collection of FAQs:
https://www.watchguard.com/support/advancedfaqs/proxy_main.asp

Protocol Anomaly Detection

As attackers become more sophisticated, new tools are necessary to counter their threats. Anomaly detection is a powerful new technology for protecting your network from attacks.

An anomaly—in the context of network security—is data, action, or behavior that deviates from what is expected for a given user, network, or system. Because network protocols are normally very restrictive, strict models of expected behavior can be constructed and deviations easily noted. Protocol anomaly detection (PAD) can detect a wide range of anomalies within the protocol space.

Using protocol anomaly detection, you can automatically add originators of malformed packets to the auto-blocked sites list. You can specify the rules that determine whether a packet is malformed, such as "non-allowed query type" or "question length too long for DNS request."

Protocol anomaly detection is supported by the SMTP, FTP, and DNS proxies.

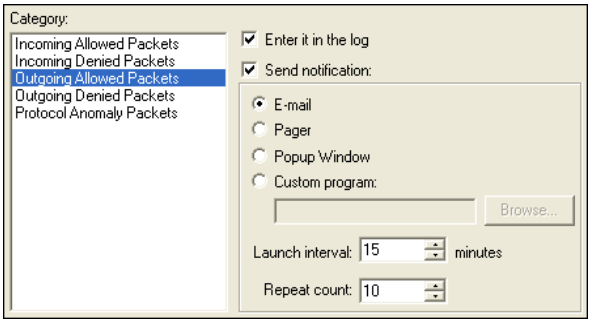
Customizing Logging and Notification for Proxies

For more information on logging and notification and the various fields on the **Logging and Notification** dialog box, see "Customizing logging and notification" on page 120.

From the **Properties** dialog box:

1 Click the **Incoming** tab.

2 Click **Logging**.
The Logging and Notification dialog box appears, as shown in the following figure.



3 Customize logging and notification using the settings in this dialog box, as described in "Customizing logging and notification" on page 120.

Configuring an SMTP Proxy Service

The SMTP proxy limits several potentially harmful aspects of email. The proxy scans the content type and content disposition headers, and then compares them against a user-defined list of known hostile signatures. Email messages containing suspect attachments are stripped of their attachments and then sent to the intended recipient.

The proxy can limit message size and limit the number of message recipients. For example, if the message exceeds preset limits for message size or number of recipients, the Firebox refuses the mail. The SMTP proxy also automatically disables non-standard commands such as DEBUG.

The following SMTP keywords are supported:

DATA	EXPN
RCPT	HELP
MAIL	RSET
QUIT	ONEX
HELO	NOOP
VRFY	QSND

The following ESMTP keywords are supported:

AUTH	CHUNKING
BDAT	EHLO
BINARYMIME	ETRN
8BITMIME	SIZE

For more information on the SMTP proxy, see the following FAQ:
https://www.watchguard.com/support/advancedfaqs/proxy_smtp.asp

Configuring the Incoming SMTP Proxy

Use the **Incoming SMTP Proxy** dialog box to set the incoming parameters of the SMTP proxy. You must already have an SMTP Proxy service icon in the Services Arena. (For information on how to add a service, see the previous chapter.) From the Services Arena:

1. Double-click the SMTP Proxy icon to open the **SMTP Properties** dialog box.
2. Click the **Properties** tab.
3. Click **Incoming**.
   The Incoming SMTP Proxy dialog box appears, displaying the General tab.
4. Modify properties on the **General** tab according to your preferences.
   For a description of each control, right-click it, and then select What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

Configuring ESMTP

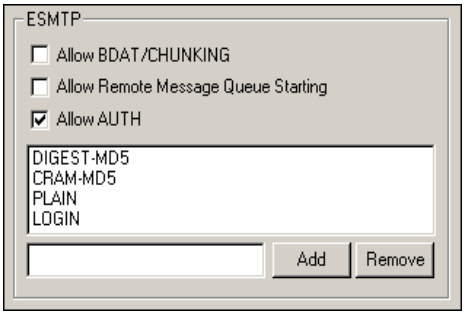
ESMTP (Extended Simple Mail Transfer Protocol) provides extensions to SMTP for sending email that supports graphics, audio and video files, and text in various foreign languages. You use the **ESMTP** tab on the **Incoming SMTP Proxy** dialog box to specify support for ESMTP extensions (keywords) and for entering AUTH types, which specify various ways of authenticating to the SMTP server.

From the **Incoming SMTP Proxy Properties** dialog box:

1 Click the **ESMTP** tab.
The ESTMP information appears, as shown in the following figure.

2 Enable the extensions (keywords) you want by selecting their associated checkboxes.

3 Use the text box provided to enter AUTH types. Click **Add**.
All AUTH types are supported; DIGEST-MD5, CRAM-MD5, PLAIN, and LOGIN are provided as defaults.



Blocking email attachments

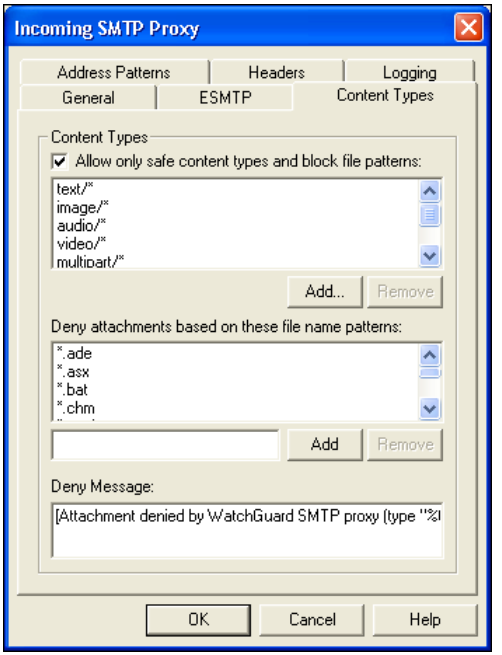
You can use two methods to block email attachments. Either allow only safe content types or deny file name patterns. These two methods can be used together to further protect your network from malicious email attachments.

Allowing safe content types

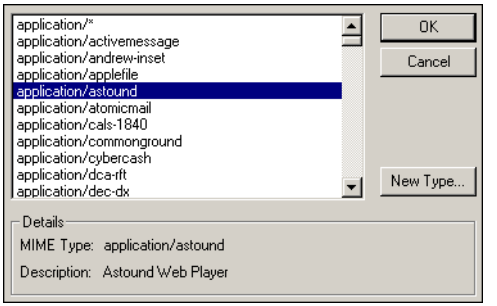
MIME stands for Multipurpose Internet Mail Extensions, a specification about how to pass audio, video, and graphics content by way of email or HTML. The MIME format attaches a header to content. The header describes the type of multimedia content contained within an email or on a Web site. For instance, a MIME type of ”application/zip” in an email message indicates that the email contains a Zip file attachment. By reading the MIME headers contained in an incoming email message, the Firebox can strip certain MIME types and admit only the types you want. You define which types of attachments are admitted and which are denied by using the Firebox’s HTTP and SMTP proxies.

From the **Incoming SMTP Proxy Properties** dialog box:

1 Click the **Content Types** tab. Specify whether you want to block certain file-name patterns in email attachments by selecting the checkbox marked **Allow only safe content types and block file patterns**.



2 If you want to specify content types to allow, click the upper **Add** button in the dialog box.
The Select MIME Type dialog box appears as shown in the following figure.



3 Select a MIME type. Click **OK**.

4 To create a new MIME type, click **New Type**. Enter the MIME type and description. Click **OK**.

The new type appears at the bottom of the Content Types drop-down list. Repeat this process for each content type. For a list of MIME content types, see the Reference Guide.

You can use wildcard characters as follows:

To allow content types

An asterisk (*) matches any string, including an empty string.

To deny file name patterns:

An asterisk (*) matches any string, including an empty string.

A question mark (?) matches any single character.

Denying attachments based on file name patterns

The **Content Types** tab includes a list of file-name patterns denied by the Firebox if they appear in email attachments. To add a file-name pattern to the list, enter a new pattern in the text box to the left of the **Add** button. Click **Add**.

Note that denying a particular attachment does not automatically trigger protocol anomaly detection (PAD) rules. You must specifically add the content type to the PAD rules, as described in “Configuring the Incoming SMTP Proxy” on page 128.

Specifying a deny message

In the **Content Types** tab, you can enter a message to be shown when a content type is denied—this message is shown to the recipient only and not the sender. A default message is provided. Use the variable %t to add the content type to the message. Use the variable %f to add the file name pattern to the message.

Adding address patterns

Adding address patterns can be useful for reducing spam content. From the **Incoming SMTP Proxy Properties** dialog box:

1 Click the **Address Patterns** tab.

2 Use the **Category** drop-down list to select a category.

3 Type the address pattern in the text box to the left of the **Add** button.

4 Click **Add**.
The address pattern appears at the bottom of the pattern list.

Protecting mail servers against relaying

Hackers and spammers may attempt to use an open relay to send mail from your servers. To prevent this, disable open relay on your mail servers by restricting the destination to only your own domain.

To further increase protection from mail relaying, modify the SMTP Proxy settings to allow addresses only from your domain. From the **Incoming SMTP Proxy Properties** dialog box:

1 Click the **Address Patterns** tab.

2 Select **Allowed To** from the **Category** drop-down list.

3 In the text box to the left of the **Add** button, enter your own domain.

4 Click **Add**.

5 Save the new configuration to the Firebox.

NOTE

If your users send mail remotely through your server, they can send mail only to your domain.

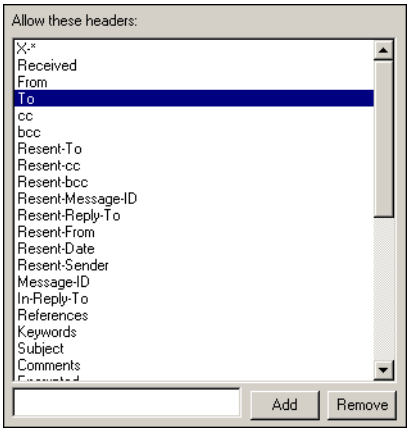
Select headers to allow

The Firebox allows certain headers by default. These are listed on the **Headers** tab of the **Incoming SMTP Proxy Properties** dialog box. You can add more headers to this list, or remove headers from the list. From the **Incoming SMTP Proxy Properties** dialog box:

1 Click the **Headers** tab.
The headers information appears, as shown in the following figure.

2 To add a new header, type the header name in the text box to the left of the **Add** button. Click **Add**.
The new header appears at the bottom of the header list.

3 To remove a header, select the header name in the header list. Click **Remove**.
The header is removed from the header list.



Specifying logging for the SMTP proxy

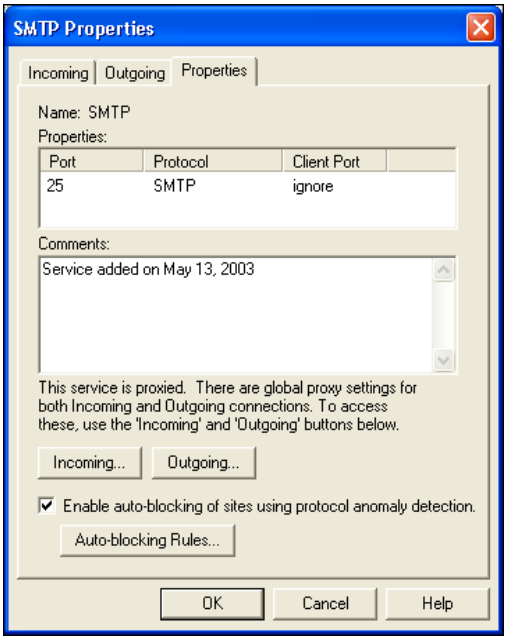
Click the **Logging** tab to specify whether to log the following:

- Unknown headers that are filtered by the proxy.
- Unknown ESMTP extensions that are filtered by the proxy.
- Accounting and auditing information.

Enabling protocol anomaly detection for SMTP

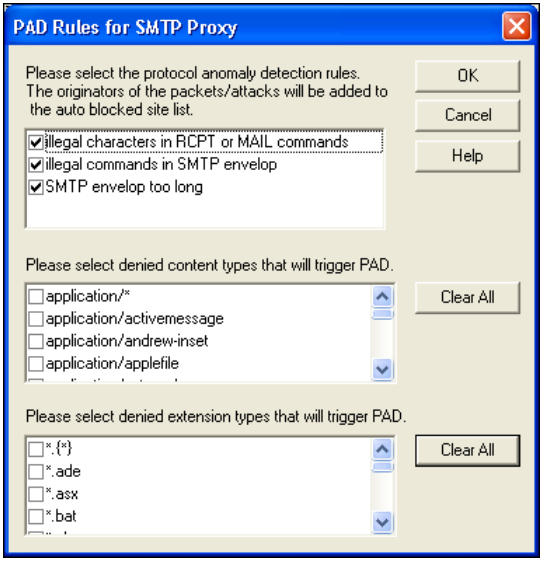
For a description of protocol anomaly detection, see “Protocol Anomaly Detection” on page 126.

1 From the **SMTP Properties** dialog box, click the **Properties** tab.
The SMTP Properties dialog box appears, as shown in the following figure.



2 Select the **Enable auto-blocking of sites using protocol anomaly detection** checkbox.

3 To set rules for anomaly detection, click the **Auto-blocking Rules** button.
The PAD Rules for SMTP Proxy dialog box appears, as shown in the following figure.



4 In the upper box, select the rules to determine which packet originators are automatically added to the auto-blocked sites list.

5 The next box lists the denied content types listed on the **Content Types** tab ("Allowing safe content types" on page 129). By default, none of these content types trigger protocol anomaly detection. If you want to enable protocol anomaly detection for these content types, select the corresponding checkbox.

To be able to select or clear several consecutive content types as a group, select the first type, press Shift and select the last type, and then select one of the types between the two selections.
To be able to select or clear several non-consecutive content types as a group, press Ctrl and select each type you want.

6 The next box lists the denied extension types listed on the **Content Types** tab ("Allowing safe content types" on page 129). By default, none of these extension types trigger protocol anomaly detection. If you want to enable protocol anomaly detection for these extensions, select the corresponding checkbox.

Configuring the Outgoing SMTP Proxy

Use the **Outgoing SMTP Proxy** dialog box to set the parameters for outgoing traffic. You must already have an SMTP Proxy service icon in the Services Arena to use this functionality. Double-click the icon to open the service's **Properties** dialog box:

1 Click the **Properties** tab.

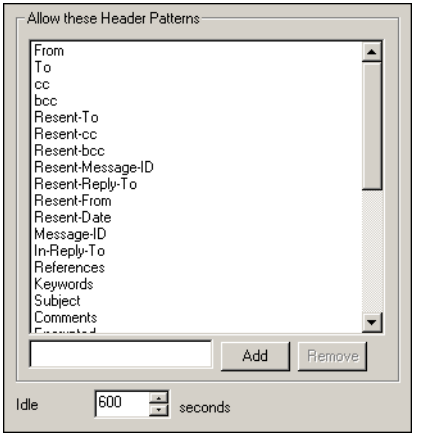
2 Click **Outgoing**.
The Outgoing SMTP Proxy dialog box appears, displaying the General tab, as shown in the following figure.

3 To add a new header pattern, type the pattern name in the text box to the left of the **Add** button. Click **Add**.

4 To remove a header from the pattern list, click the header pattern. Click **Remove**.

5 In the **Idle** field, set a time-out value in seconds.

6 To modify logging properties, click the **Logging** tab and set the options you want.



NOTE

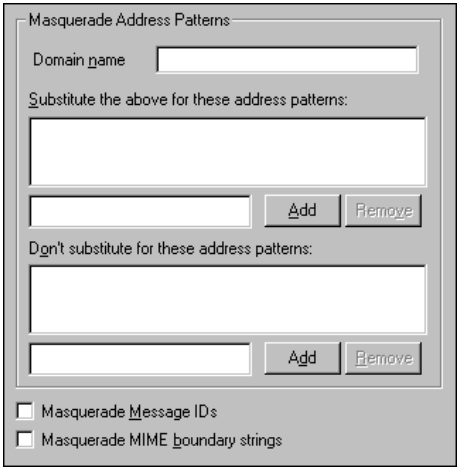
If you send large volumes of email, it is good practice to set outgoing to Disabled. This filters outgoing mail and puts less load on the Firebox.

Add masquerading options

SMTP masquerading converts an address pattern behind the firewall into an anonymous, public address. For example, the

internal address pattern might be inside.salesdept.bigcompany.com, which would become the public address `bigcompany.com`.

1 Click the **Masquerading** tab.
The SMTP masquerading information appears, as shown in the following figure.



2 Enter the official domain name.
This is the name you want visible to the outside world.

3 In the **Substitute the above for these address patterns** text box (to the left of the **Add** button), type the address patterns that are behind your firewall that you want replaced by the official domain name. Click **Add**.
All patterns entered here appear as the official domain name outside the Firebox.

4 In the **Don't Substitute for these address patterns** text box (to the left of the **Add** button), type the address patterns that you want to appear "as is" outside the firewall. Click **Add**.

5 Select the checkbox marked **Masquerade Message IDs** to specify that message IDs in the Message-ID and Resent-Message-ID header fields are converted to a new ID composed of an encoded version of the original ID, a time stamp, and the host name entered in the domain name field described in step 2.

6 Select the checkbox marked **Masquerade MIME boundary strings** to specify that the firewall converts MIME boundary strings in messages and attachments to a string that does not reveal internal host names or other identifying information.

Configuring an FTP Proxy Service

The FTP proxy service enables you to access another computer (on a separate network) for the purposes of browsing directories and copying files. Consequently, FTP is inherently dangerous. If configured incorrectly, the FTP service allows intruders to access your network and important information such as passwords and configuration files. FTP is also potentially dangerous outbound because it enables users on your network to copy virtually anything from outside the network to a location behind their firewall.

Therefore, it is important to make the FTP service as restrictive as possible. Ideally, try to isolate the inbound FTP servers to a single host (or hosts) on your optional interface or on one of the less trusted ports. Make sure you protect your trusted network from FTP requests from the host or hosts on other networks as well. Like SMTP, the FTP proxy includes customized features that provide more complete control over the traffic that passes through your firewall.

For detailed information about the FTP proxy, see the following FAQ:

https://www.watchguard.com/support/advancedfaqs/proxy_ftp.asp

For troubleshooting information for the FTP proxy, see the following FAQ:

https://www.watchguard.com/support/advancedfaqs/proxy_ftptrouble.asp

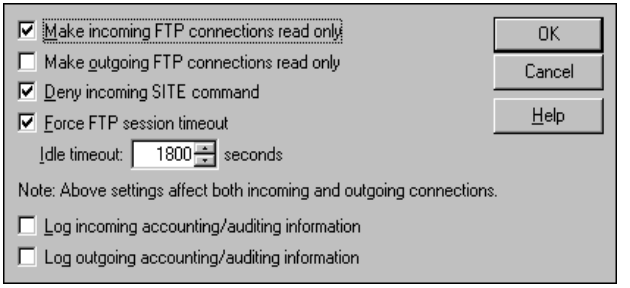
From Policy Manager:

1 If you have not done so already, use the **Add Service** button to add the FTP proxy service. Expand the Proxies tree and double-click the FTP service icon.

2 Click the **Properties** tab. Click **Settings**.
The Settings information appears as shown in the following figure.

3 Enable FTP proxy properties according to your security policy preferences.
For a description of each control, right-click it, and then select What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.
Note that the Make Incoming FTP Connections Read only checkbox is selected by default. If you have an FTP server that accepts files, be sure to clear this checkbox. If you do not, the stor command cannot be sent.

4 Click **OK**.



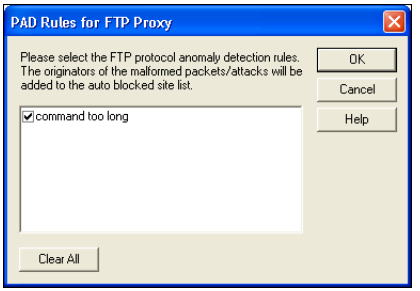
Enabling protocol anomaly detection for FTP

For a description of protocol anomaly detection, see "Protocol Anomaly Detection" on page 126.

1 From the **FTP Properties** dialog box, click the **Properties** tab.

2 Select the **Enable auto-blocking of sites using protocol anomaly detection** checkbox.

3 To set rules for anomaly detection, click the **Auto-blocking Rules** button.
The PAD Rules for FTP Proxy dialog box appears.


PAD Rules for FTP Proxy
Please select the FTP protocol anomaly detection rules. The originators of the malformed packets/attacks will be added to the auto blocked site list.
OK
Cancel
Help
command too long
Clear All

4 Select the rules to determine which packet originators are automatically added to the auto-blocked sites list.

Selecting an HTTP Service

Because of the extensive security implications of HTTP traffic, it is important to restrict the incoming service as much as possible. Many administrators set up public Web servers only on their optional interface or one of the less trusted ports. They restrict incoming HTTP traffic to the optional interface and prohibit incoming HTTP traffic from traveling from a less trusted port to a more trusted port. Outgoing traffic is generally less restrictive. For example, many companies open outgoing HTTP traffic from Any to Any.

WatchGuard System Manager offers three different types of HTTP services. Choose the HTTP service that best meets your needs:

- **Proxied-HTTP** is a multiservice that combines configuration options for HTTP on port 80 with a rule that allows (by default) all outgoing TCP connections. In other words, the Proxied-HTTP is not bilateral incoming and outgoing; this service controls incoming TCP traffic only on port 80, but allows outgoing TCP traffic on all ports. The Proxied-HTTP service includes a variety of custom options including specialized logging features, definition of safe content types, and WebBlocker. Because this routes all outgoing TCP connections, it can interface with non-HTTP traffic. If you are unsure, use HTTP instead.

- **HTTP** is a proxy service that functions very much like Proxied-HTTP, except that it controls both incoming and outgoing access only on port 80.

NOTE

The WatchGuard service called "HTTP" is not to be confused with an HTTP caching proxy. An HTTP caching proxy refers to a separate machine that performs caching of Web data.

- **Filtered-HTTP** is a multiservice that combines configuration options for HTTP on port 80 with a rule allowing (by default) all outgoing TCP connections. As a filtered service, Filtered-HTTP is considerably faster than Proxied-HTTP or HTTP, but does not provide protection that is as thorough or as effective. In addition, none of the custom options, including WebBlocker, are available for Filtered-HTTP.

Adding a proxy service for HTTP

Most network administrators use the HTTP proxy service when configuring Web traffic. Many administrators combine their HTTP service with an outgoing proxy service configured Any to Any to keep the HTTP service both easy to understand and control. In the following procedure, you define the content allowed to pass through the firewall.

1. In Policy Manager, click the **Add Service** icon. Expand the **Proxies** folder, double-click **HTTP**, and then click **OK**.
   The HTTP Properties dialog box appears. The default stance is to deny incoming traffic and to allow outgoing traffic from Any to Any.
2. Use the **Incoming HTTP connections are** drop-down list to select **Enabled and Allowed**.
3. Configure the service as you want. For example, to configure the HTTP proxy to allow incoming traffic from Any to the optional network or to a less trusted port, click **Add** beneath the **To** list. In the **Add Address** dialog box, add the **optional** Firebox group. Click **OK**.
4. Click the **Properties** tab. Click **Settings**.
5. On the **Settings** tab, enable HTTP proxy properties according to your security policy preferences.

6 If you are using the HTTP proxy service because you want to use WebBlocker, see Chapter 16, “Controlling Web Site Access.”

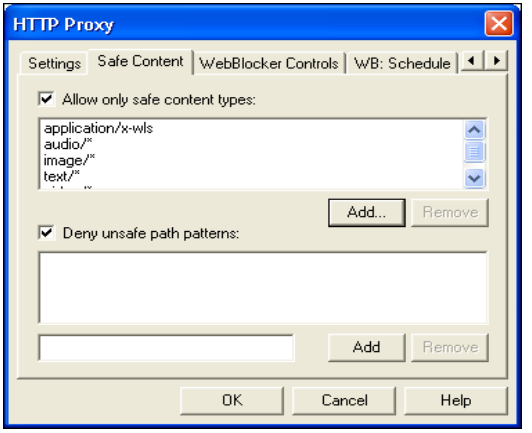
For a description of each control, right-click it, and then select What's This?. Or, refer to the Field Definitions chapter in the Reference Guide.

For detailed information about the HTTP proxy, see the online support resources at http://www.watchguard.com/support.

Restricting content types for the HTTP proxy

You can configure the HTTP proxy to allow only those MIME types you decide are acceptable security risks. On the **Safe Content** tab:

1 To specify that you want to restrict content types that can pass through the HTTP proxy, select the checkbox marked **Allow only safe content types**.



2 If you want to specify content types to allow, click the upper **Add** button in the dialog box.

The Select MIME Type dialog box appears.

3 Select a MIME type. Click **OK**.

4 To create a new MIME type, click **New Type**. Enter the MIME type and description. Click **OK**.

The new type appears at the bottom of the Content Types drop-down list. Repeat this process for each content type. For a list of MIME content types, see the Reference Guide.

5 If you want to specify unsafe path patterns to block, enter a path pattern next to the left of the **Add** button. Click **Add**.
Only the path and not the host name are filtered. For example, with the Web site www.testsite.com/login/here/index.html, only the elements /login/ and /here/ can be added to the unsafe path patterns box, not *testsite*.

NOTE

Zip files are denied when you deny Java or ActiveX applets, because Zip files often contain these applets.

Configuring a caching proxy server

Because the Firebox's HTTP proxy does no content caching, the Firebox has been designed to work with caching proxy servers. Because company employees often visit the same Web sites, this greatly speeds operations and reduces the load on external Internet connections. All Firebox proxy and WebBlocker rules that are in place still have the same effect.

The Firebox communicates with proxy servers exactly the same way that clients normally do. Instead of a GET request from the Firebox to the Internet looking like this:

```
GET / HTTP/1.1
```

It ends up looking like this, and the request is sent to the configured caching proxy server instead:

```
GET www.mydomain.com / HTTP/1.1
```

The proxy server then forwards this request to the Web server mentioned in the GET request.

To set up an external caching proxy server:

1 Configure an external proxy server, such as Microsoft Proxy Server 2.0.

2 Open Policy Manager with your current configuration.

3 Double-click the icon for your HTTP proxy service.
This can be either Proxy, HTTP, or Proxied-HTTP.

4 Click the **Properties** tab. Click the **Settings** button.

5 Select the checkbox marked **Use Caching Proxy Server**.

6 In the fields below the checkbox, enter the IP address and TCP port of the caching proxy server. Click **OK**.

7 Save this configuration to the Firebox.

Configuring the DNS Proxy Service

Internet domain names (such as WatchGuard.com) are located and translated into IP addresses by the domain name system (DNS). DNS lets users navigate the Internet with easy-to-remember “dot-com” names by seamlessly translating the domain name into an IP address that servers, routers, and individual computers understand. Rather than try to maintain a centralized list of domain names and corresponding IP addresses, smaller lists are distributed across the Internet.

The Berkeley Internet Name Domain (BIND) is a widely used implementation of DNS. Some versions of BIND can be vulnerable to attacks that cause a buffer overflow, which crash the targeted server and enable the attacker to gain unauthorized access to your network.

One attack uses a flaw in the transaction signature (TSIG) handling code. When BIND encounters a request with a valid transaction signature but no valid key, processing steps that initialize important variables (notably the required buffer size) are skipped. Subsequent function calls make invalid assumptions about the size of the request buffer, which can cause requests with legitimate transaction signatures and keys to trigger a buffer overflow. Used in conjunction with other attack tools, this type of attack results in a server crash and the attacker gaining unauthorized access to your root shell through an outbound TCP connection. Using this connection, the attacker can execute arbitrary code on your network.

Some versions of BIND are also vulnerable to another type of buffer overflow attack that exploits how NXT (or next) records are processed. Attackers can set the value of a key variable such that the server crashes and the attacker gains unauthorized access. The DNS proxy protects your DNS servers from both the TSIG and NXT attacks, along with a number of other types of DNS attacks. For more information on the DNS proxy, see the DNS Proxy section of the following collection of FAQs: https://www.watchguard.com/support/advancedfaqs/proxy_main.asp

NOTE

Unless you have a DNS server for public use, you should not use this proxy.

Adding the DNS Proxy Service

When you add the DNS proxy, you can best protect your network by applying the proxy to both inbound and outbound traffic. You can also set up the DNS proxy so that any denied packets (inbound or outbound) generate log records. You can use LogViewer to check your log files for records that indicate DNS attacks, which in turn lets you see how often and from where you were attacked.

1 On the toolbar, click the Add Services icon.

2 Expand the **Proxies** folder.
A list of pre-configured proxies appears.

3 Click **DNS-Proxy**. Click **Add**.
The Add Service dialog box appears. You can change the name assigned to the DNS proxy or change the comment associated with the proxy.

4 Click **OK** to close the **Add Service** dialog box.
The DNS-Proxy Properties dialog box appears.

5 Click the **Incoming** tab. Use the **Incoming DNS-Proxy connections are** drop-down list to select **Enabled and Allowed**.

6 Click the **Outgoing** tab. Use the **Outgoing DNS-Proxy connections are** drop-down list to select **Enabled and Allowed**.

7 Click **OK** to close the **DNS-Proxy Properties** dialog box. Click **Close**.
The Services dialog box closes. The DNS-Proxy icon appears in the Services Arena.

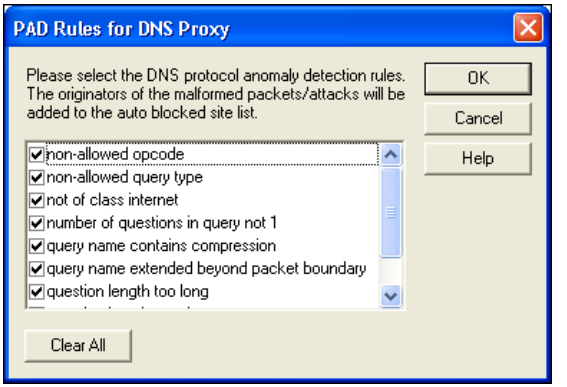
Enabling protocol anomaly detection for DNS

For a description of protocol anomaly detection, see "Protocol Anomaly Detection" on page 126.

1 From the **DNS Properties** dialog box, click the **Properties** tab.

2 Select the **Enable auto-blocking of sites using protocol anomaly detection** checkbox.

3 To set rules for anomaly detection, click the **Auto-blocking Rules** button.
The PAD Rules for DNS Proxy dialog box appears, as shown in the following figure.


PAD Rules for DNS Proxy
Please select the DNS protocol anomaly detection rules. The originators of the malformed packets/attacks will be added to the auto blocked site list.
OK
Cancel
Help
non-allowed opcode
non-allowed query type
not of class internet
number of questions in query not 1
query name contains compression
query name extended beyond packet boundary
question length too long
Clear All

4 By default, all rules are enabled. You can enable or disable the rules to determine which packet originators are automatically added to the auto-blocked sites list.
To be able to select or clear several consecutive rules as a group, select the first rule, press Shift and select the last rule, and then select one of the rules between the two selections.
To select or clear several non-consecutive rules as a group, press Ctrl and select each rule you want.

DNS file descriptor limit

The DNS proxy has only 256 file descriptors available for its use, which limits the number of DNS connections in a NAT environment. Every UDP request that uses dynamic NAT uses a file descriptor for the duration of the UDP timeout. Every TCP session that uses dynamic, static, or 1-to-1 NAT uses a file descriptor for the duration of the session.

The file descriptor limit is rarely a problem, but an occasional site may experience slow name resolution and many instances of the following log message:

```
dns-proxy[xx] dns_setup_connect_udp: Unable to create UDP socket for port: Invalid argument
```

You can work around this problem in two ways (the first method is the most secure):

- Avoid using dynamic NAT between your clients and your DNS server.
- Disable the outgoing portion of the DNS proxied service and replace it with a filtered DNS service.

CHAPTER 10

Creating Aliases and Implementing Authentication

Aliases are shortcuts used to identify groups of hosts, networks, or users. The use of aliases simplifies service configuration.

User authentication allows the tracking of connections based on name rather than IP address. With authentication, it does not matter which IP address is used or from which machine a person chooses to work. To gain access to Internet services (such as outgoing HTTP or outgoing FTP), the user provides authenticating data in the form of a username and password. For the duration of the authentication, the session name is tied to connections originating from the IP address from which the individual authenticated. This makes it possible to track not only the machines from which connections are originating, but the user as well.

NOTE

Because usernames are bound to IP addresses, user authentication is not recommended for use in an environment with shared multiuser machines (such as Unix, Citrix, or NT terminal servers), because only one user per shared server can be authenticated at any one time.

The Firebox allows you to define permissions and groups using user names rather than IP addresses. This system allows for situations where users may use more than one computer or IP

address. Tracking activities by user rather than IP is especially useful on networks using DHCP where a user workstation may have several different IP addresses over the course of a week. Authentication by user is also useful in education environments, such as classrooms and college computer centers where many different people might use the same IP address over the course of the day. For more information on authentication, see the following collection of FAQs:
https://www.watchguard.com/support/advancedfaqs/auth_main.asp

Using Aliases

Aliases provide a simple way to remember host IP addresses, host ranges, and network IP addresses. They function in a similar fashion to email distribution lists—combining addresses and names into easily recognizable groups. Use aliases to quickly build service filter rules. Aliases cannot, however, be used to configure the network itself.

WatchGuard automatically adds six aliases to the basic configuration:

Group	Function
firebox	Addresses assigned to the three Firebox interfaces and any related networks or device aliases
trusted	Any host or network routed through the physical trusted interface
optional	Any host or network routed through the physical optional interface
external	Any host or network routed through the physical external interface; in most cases, the Internet
dvcp_nets	Networks at the other end of a VPN tunnel
dvcp_local_nets	Networks behind the Firebox being configured

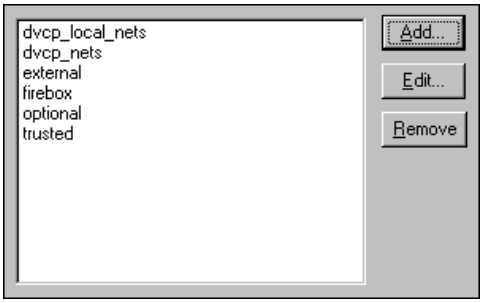
If you have purchased the Firebox X 3-Port Upgrade, the aliases eth3, eth4, and eth5 are also added.

A host alias takes precedence over a Windows NT or RADIUS group with the same name.

Adding an alias

From Policy Manager:

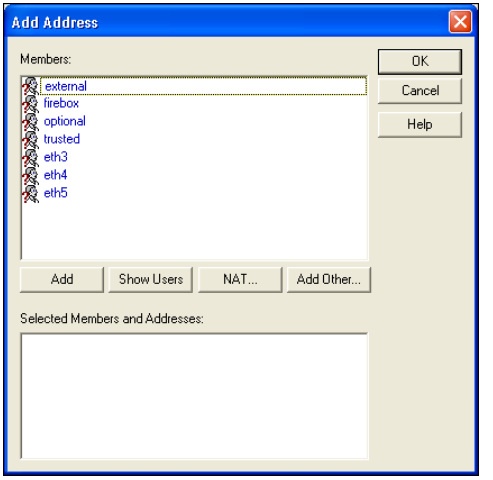
1 Select **Setup** ⇒ **Aliases**.
The Aliases dialog box appears, as shown in the following figure.



2 Click **Add**.

3 In the **Host Alias Name** text box, enter the name used to identify the alias when configuring services and authentication.

4 Click **Add**.
The Add Address dialog box appears, as shown in the following figure.



5 Define the alias by adding members. To add an existing member, click the name in the **Members** list. Click **Add**.

6 To configure a new member, click **Add Other**.
The Add Member dialog box appears.

7 Use the **Choose Type** drop-down list to select a category. In the **Value** text box, enter the address, range, or host name. Click **OK**.

8 When you finish adding members, click **OK**.
The Host Alias dialog box appears listing the new alias. Click the alias to view its members.

To modify an alias, select it, click **Edit,** and then add or delete members.

To remove an alias, select it, click **Remove**, and then remove the alias from **Properties** box of any services configured to use the alias. For more information, see "Defining Service Properties" on page 117.

How User Authentication Works

A specialized HTTP server runs on the Firebox. To authenticate, clients must connect to the authentication server using a Java-enabled Web browser pointed to:
http://*IP address of any Firebox interface*:4100/

A Java applet loads a prompt for a username and password that it then passes to the authentication server using a challenge-response protocol. Once successfully authenticated, users minimize the Java applet and browser window and begin using allowed network services.

As long as the Java window remains active (it can be minimized but not closed) and the Firebox does not reboot, users remain authenticated until the session times out. To prevent an account from authenticating, disable the account on the authentication server.

Using external authentication

Although the authentication applet is primarily used for outbound traffic, it can be used for inbound traffic as well. Authentication can be used outside the Firebox as long as you have an account on that Firebox. For example, if you are work-

ing at home, you can point your browser to:
http://*public IP address of any Firebox interface*:4100/

The authentication applet appears to prompt you for your login credentials. This can provide you access through various services such as FTP and Telnet, if you have preconfigured your Firebox to allow this.

Enabling remote authentication

Use this procedure to allow remote users to authenticate from the external interface, which gives them access to services through the Firebox.

1. In the Services Arena in Policy Manager, double-click the wg_authentication service icon.
2. On the **Incoming** tab, select **Enabled and Allowed**.
3. Under the **From** box, click **Add**.
4. Click **Add Under** and add the IP addresses of the remote users you are allowing to authenticate externally.

Authenticating from optional networks

1. In the Services Arena in Policy Manager, double-click the wg_authentication service icon.
2. On the **Incoming** tab, select **Enabled and Allowed**.
3. Under the **From** box, click **Add**.
4. Click **Add Under** and add the IP address, user, or group you are allowing to authenticate from an optional network.

Authentication Server Types

WatchGuard System Manager can authenticate users against any of five authentication server types:

- A built-in authentication server on the Firebox
- NT primary domain controllers
- RADIUS-compliant authentication servers
- CRYPTOCard authentication servers
- SecurID authentication servers

The differences among the various authentication schemes are essentially transparent to the user; the user performs many or all

of the same tasks to authenticate against any of the five types of authentication.

The difference for the Firebox administrator is that for built-in authentication, the database of usernames, passwords, and groups are stored on the Firebox itself. In all other cases, the usernames, passwords, and groups are stored on the server performing the authentication.

When the Firebox is not the authentication server, you must set up the authentication server according to the manufacturer's instructions and place it on the network in a location accessible to the Firebox. It is best placed on the trusted side for security reasons.

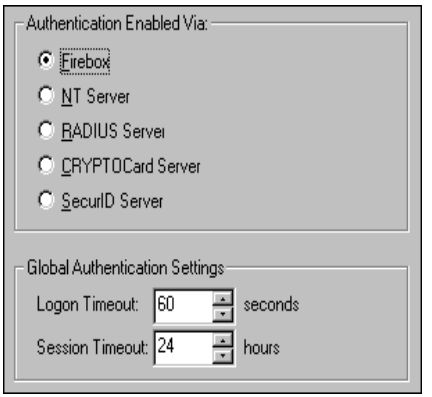
To specify authentication type:

1 From Policy Manager, select **Setup ⇒ Firewall Authentication**.
The Firewall Authentication dialog box appears, as shown in the following figure.

2 In the **Authentication Enabled Via** box, select the authentication server you want you use.

3 In **Logon Timeout**, select how many seconds are allowed for an attempted logon before the time-out shuts down the connection.

4 In **Session Timeout**, set how many hours a session can remain open before the time-out shuts down the connection. This is a set time limit regardless of end-user traffic.



Defining Firebox Users and Groups for Authentication

In the absence of a third-party authentication server, you can divide your company into groups and users for authentication. Assign employees or members to groups based on factors such as common tasks and functions, access needs, and trustworthiness. For example, you might have a group for accounting, another for marketing, and a third for research and development. You also might create a probationary group with high restrictions for new employees.

Within groups, you define users according to factors such as the method they use to authenticate, the type of system they use, or the information they need to access. Users can be either networks or individual computers. As your organization changes, you can add or remove users or systems from groups.

NOTE

You can define only a limited number of Firebox users. If you have more than approximately 100 users to authenticate, WatchGuard recommends that you use a third-party authentication server.

WatchGuard automatically adds two groups—intended for remote users—to the basic configuration file:

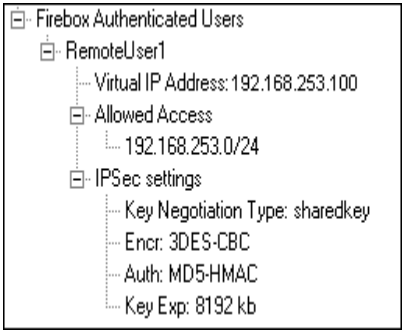
ipsec_users
Add the names of authorized users of MUVPN.

pptp_users
Add the names of authorized users of RUVPN with PPTP.

You can use Policy Manager to add, edit, or delete other groups to or from the configuration file or to add or modify the users within a group.

From Policy Manager:

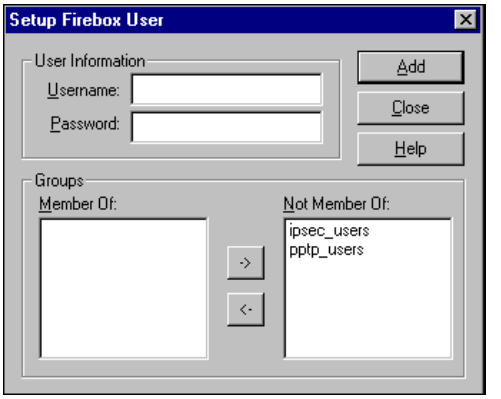
1 Select **Setup ⇒ Authentication Servers**.
The Authentication Servers dialog box appears, as shown in the following figure.



2 To add a new group, click the **Add** button beneath the **Groups** list.
The Add Firebox Group dialog box appears.

3 Type the name of the group. Click **OK**.

4 To add a new user, click the **Add** button beneath the **Users** list.
The Setup Firebox User dialog box appears, as shown in the following figure.



5 Enter the username and password.

6 To add the user to a group, select the group name in the **Not Member Of** list. Click the left-pointing arrow to move the name to the **Member Of** list.

7 When you finish adding the user to groups, click **Add**.
The user is added to the User list. The Setup Firebox User dialog box remains open and cleared for entry of another user.

8 To close the **Setup Firebox User** dialog box, click **Close**.
The Firebox Users tab appears with a list of the newly configured users.

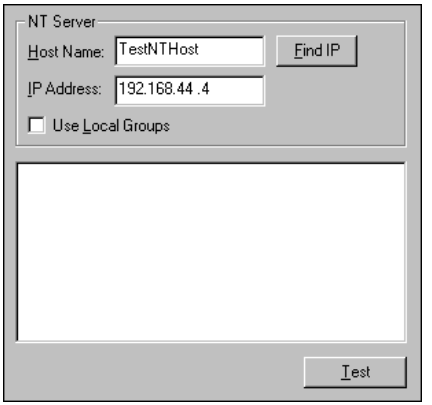
9 When you finish adding users and groups, click **OK**.
The users and groups can now be used to configure services and authentication.

Configuring Windows NT Server Authentication

Windows NT Server authentication is based on Windows NT Server Users and Groups. It uses the Users and Groups database already in place on your Windows NT network. Only end users are allowed to authenticate; the default Windows NT groups Administrators and Replicators will not authenticate using this feature. From Policy Manager:

1 Select **Setup ⇒ Authentication Servers**.
The Authentication Servers dialog box appears.

2 Click the **NT Server** tab.
The information appears as shown in the following figure.



3 To identify the host, enter both the host name and the IP address of the Windows NT network. If you don't know the IP address of the host, click **Find IP**. The IP address is automatically entered.
When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

4 If you want, select the checkbox to use local groups.
Windows NT defines two types of groups: global and local. A local group is local to the security system in which it is created. Global groups contain user accounts from one domain grouped together as one group name. A global group cannot contain another global group or a local group.

5 Click **OK**.

Configuring RADIUS Server Authentication

The Remote Authentication Dial-In User Service (RADIUS) provides remote users with secure access to corporate networks. RADIUS is a client-server system that stores authentication information for users, remote access servers, and VPN gateways in a central user database that is available to all clients. Authentication for the entire network occurs from one location.

RADIUS prevents hackers from intercepting and responding to authentication requests because authentication requests transmit an authentication key that identifies it to the RADIUS server. Note that it is the key that is transmitted, and not a password. The key resides on the client and server simultaneously, which is why it is often called a "shared secret."

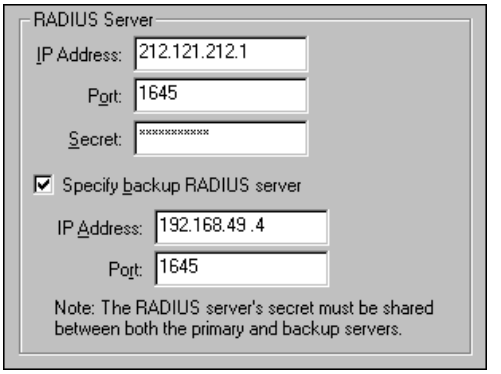
To add or remove services accessible by RADIUS authenticated users, add the RADIUS user or group in the individual service properties dialog box and the IP address of the Firebox on the RADIUS authentication server.

Although WatchGuard supports both CHAP and PAP authentication, CHAP is considered more secure.

From Policy Manager:

1 Select **Setup ⇒ Authentication Servers**.
The Authentication Servers dialog box appears.

2 Click the **RADIUS Server** tab.
The RADIUS information appears, as shown in the following figure.


RADIUS Server
IP Address: 212.121.212.1
Port: 1645
Secret: **********
Specify backup RADIUS server
IP Address: 192.168.49 .4
Port: 1645
Note: The RADIUS server's secret must be shared between both the primary and backup servers.

3 Enter the IP address of the RADIUS server.

4 Enter or verify the port number used for RADIUS authentication.
The default is 1645. RFC 2138 states the port number as 1812, but many RADIUS servers still use port number 1645.

5 Enter the value of the secret shared between the Firebox and the RADIUS server.
The shared secret is case-sensitive and must be identical on the Firebox and the RADIUS server.

6 Enter the IP address and port of the backup RADIUS server. The RADIUS servers' secret must be shared between both the primary and backup servers.

7 Click **OK**.

8 Gather the IP address of the Firebox and the user or group aliases you want to authenticate using RADIUS. The aliases appear in the **From** and **To** listboxes for the individual services.

To configure the RADIUS server

1 Add the IP address of the Firebox where appropriate according to the RADIUS server vendor.
Some RADIUS vendors may not require this. To determine if this is required for your implementation, check the RADIUS server vendor documentation.

2 Take the user or group aliases gathered from the **Add Address** dialog box from each service (double-click the service icon, select **Incoming and Allowed** on the **Incoming**

tab, and click **Add**) and add them to the defined Filter-IDs in the RADIUS configuration file. For more information, consult the RADIUS server documentation.

For example, to add the groups Sales, Marketing, and Engineering enter:
Filter-Id="Sales"
Filter-Id="Marketing"
Filter-Id="Engineering"

NOTE

The filter rules for RADIUS user filter-IDs are case sensitive.

Configuring CRYPTOCard Server Authentication

CRYPTOCard is a hardware-based authentication system that allows users to authenticate by way of the CRYPTOCard challenge response system which includes off-line hashing of passwords. It enables you to authenticate individuals independent of the hosts they are on.

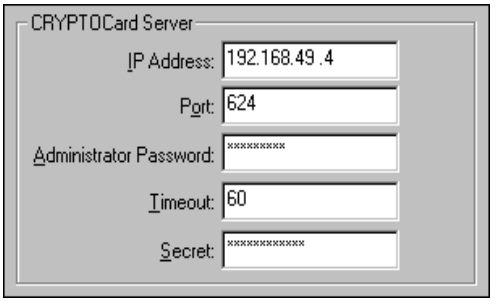
Configuring WatchGuard CRYPTOCard server authentication assumes that you have acquired and installed a CRYPTOCard server according to the manufacturer's instructions, and that the server is accessible for authentications to the Firebox.

To add or remove services accessible by CRYPTOCard authenticated users, add the CRYPTOCard user or group in the individual service's **Properties** dialog box, and the IP address of the Firebox on the CRYPTOCard authentication server.

From Policy Manager:

1 Select **Setup** ⇒ **Authentication Servers**.
The Authentication Servers dialog box appears.

2 Click the **CRYPTOCard Server** tab.
You might need to use the arrow buttons in the upper-right corner of the dialog box to bring this tab into view.



3 Enter the IP address of the CRYPTOCard server.

4 Enter or verify the port number used for CRYPTOCard authentication.
The standard is 624.

5 Enter the administrator password.
This is the administrator password in the passwd file on the CRYPTOCard server.

6 Enter or accept the time-out in seconds.
The time-out period is the maximum amount of time, in seconds, a user can wait for the CRYPTOCard server to respond to a request for authentication. Sixty seconds is CRYPTOCard's recommended time-out length.

7 Enter the value of the shared secret between the Firebox and the CRYPTOCard server.
This is the key or client key in the "Peers" file on the CRYPTOCard server. This key is case-sensitive and must be identical on the Firebox and the CRYPTOCard server for CRYPTOCard authentication to work.

8 Click **OK**.

9 Gather the IP address of the Firebox and the user or group aliases to be authenticated by way of CRYPTOCard. The aliases appear in the **From** and **To** listboxes in the individual services' **Properties** dialog boxes.

On the CRYPTOCard server:

1 Add the IP address of the Firebox where appropriate according to CRYPTOCard's instructions.

2 Take the user or group aliases from the service properties listboxes and add them to the group information in the

CRYPTOCard configuration file. Only one group can be associated with each user.

For more information, consult the CRYPTOCard server documentation.

Configuring SecurID Authentication

For SecurID authentication to work, the RADIUS and ACE/Server servers must first be correctly configured. In addition, users must have a valid SecurID token and PIN number. Please see the relevant documentation for these products.

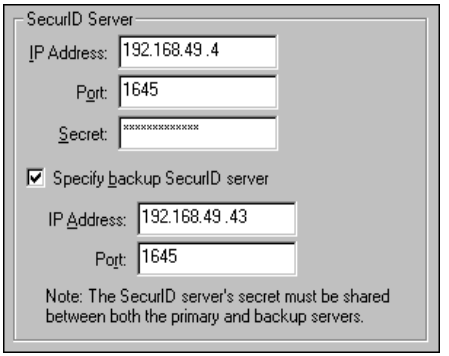
NOTE

WatchGuard does not support the third-party program Steel Belted RADIUS for use with SecurID. You should use the RADIUS program bundled with the RSA SecurID software.

From Policy Manager:

1 Select **Setup ⇒ Authentication Servers**.
The Authentication Servers dialog box appears.

2 Click the **SecurID Server** tab.
You might need to use the arrow buttons in the upper-right corner of the dialog box to bring this tab into view.



3 Enter the IP address of the SecurID server.

4 Enter or verify the port number used for SecurID authentication.
The default is 1645.

5 Enter the value of the secret shared between the Firebox and the SecurID server.

The shared secret is case-sensitive and must be identical on the Firebox and the SecurID server.

6 If you are using a backup server, select the **Specify backup SecurID server** checkbox. Enter the IP address and port number for the backup server.

7 Click **OK**.

To set up the RADIUS server, see "To configure the RADIUS server" on page 159.

CHAPTER 11

Intrusion Detection and Prevention

WatchGuard System Manager can protect your network from many types of attacks. In addition to the protection provided through filtered and proxied services, the Firebox also gives you the following tools to stop attacks that services are not designed to defeat.

Default packet handling
Options for how the firewall handles incoming communications that appear to be attacks on a network.

Blocked sites
An IP address outside the Firebox that is prevented from connecting to hosts behind the Firebox. The Blocked Sites feature of the Firebox helps you prevent unwanted contact from known or suspected hostile systems.

Blocked ports
Ports that are designated as vulnerable entry points to your network. A blocked port setting blocks packets that enter your network through the external interface.

Default Packet Handling

WatchGuard System Manager provides default packet handling options to automatically block hosts that originate probes and

attacks. Logging options help you identify sites that exhibit suspicious behavior such as spoofing. You can use the information gathered to manually and permanently block an offending site. In addition, you can block ports (by port number) to protect ports with known vulnerabilities from any incoming traffic. For more information on log messages, see the following collection of FAQs:
https://www.watchguard.com/support/advancedfaqs/log_main.asp

WatchGuard System Manager examines and handles packets according to default packet-handling options that you set. The firewall examines the source of the packet and its intended destination by IP address and port number. It also watches for patterns in successive packets that indicate unauthorized attempts to access the network.

The default packet-handling configuration determines whether and how the firewall handles incoming communications that appear to be attacks on a network. Packet handling can:

- Reject potentially threatening packets
- Automatically block all communication from a source site
- Add an event to the log
- Send notification of potential security threats

Blocking spoofing attacks

One method that attackers use to gain access to your network involves creating an electronic "false identity." With this method, called "IP spoofing," the attacker creates a TCP/IP packet that uses someone else's IP address. Because routers use a packet's destination address to forward the packet toward its destination, the packet's source address is not validated until the packet reaches its destination. In conjunction with the false identity, the attacker may route the packet so that it appears to originate from a host that the targeted system trusts.

If the destination system performs session authentication based on a connection's IP address, the destination system may allow the packet with the spoofed address through your firewall. The destination system "sees" that the packet apparently originated

from a host that is trusted, and therefore doesn't require validation or a password.

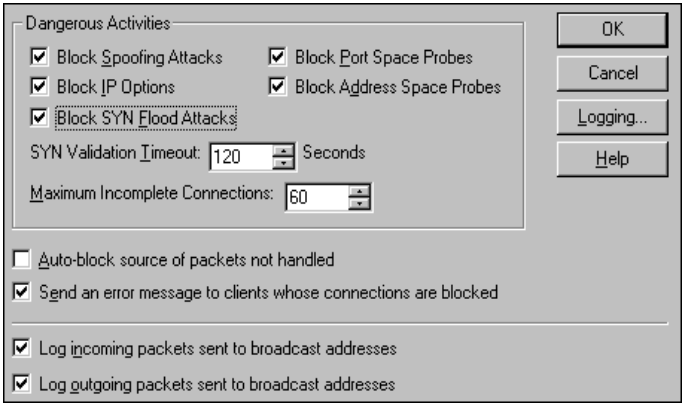
When you enable spoofing defense, the Firebox prevents packets with a false identity from passing through to your network. When such a packet attempts to establish a connection, the Firebox generates two log records. One log record shows that the attacker's packet was blocked; the other shows that the attacker's site has been added to the Blocked Sites list, a compilation of all sites blocked by the Firebox.

You can block spoofing attacks using the **Default Packet Handling** dialog box. From Policy Manager:



1 On the toolbar, click the Default Packet Handling icon, shown at right.
You can also, from Policy Manager, select Setup ⇒Intrusion Prevention ⇒ Default Packet Handling.
The Default Packet Handling dialog box appears, as shown in the following figure.

2 Select the checkbox marked **Block Spoofing Attacks**.



Blocking port space and address space attacks

Other methods that attackers use to gain access to networks and hosts are known as probes. Port space probes are used to scan a host to find what services are running on it. Address

space probes scan a network to see which services are running on the hosts inside that network. From Policy Manager:

1 On the toolbar, click the Default Packet Handling icon.
You can also, from Policy Manager, select Setup ⇒ Intrusion Prevention ⇒ Default Packet Handling.
The Default Packet Handling dialog box appears.

2 Select the checkbox marked **Block Port Space Probes**.

3 Select the checkbox marked **Block Address Space Probes**.

Stopping IP options attacks

Another type of attack that can be used to disrupt your network involves IP options in the packet header. IP options are extensions of the Internet Protocol that are usually used for debugging or for special applications. For example, if you allow IP options, the attacker can use the options to specify a route that helps him or her gain access to your network. Although there is some gain to leaving IP options enabled, the risk generally outweighs the benefit.

From Policy Manager:

1 On the toolbar, click the Default Packet Handling icon.
You can also, from Policy Manager, select Setup ⇒ Intrusion Prevention ⇒ Default Packet Handling.
The Default Packet Handling dialog box appears.

2 Select the checkbox marked **Block IP Options**.

Stopping SYN Flood attacks

A SYN Flood attack is a type of Denial of Service (DoS) attack that seeks to prevent your public services (such as email and Web servers) from being accessible to users on the Internet.

To understand how SYN Flood works, consider a normal TCP connection. A user tries to connect by way of a Web browser to your server by sending what is called a SYN segment. Your Web server acknowledges the browser by sending what is called a SYN+ACK segment. When the browser sees the SYN+ACK, it sends an ACK segment. The server is ready to accept the URL request from the browser when it sees the ACK statement. However, until the ACK segment has been received, the server is "stuck"; it knows the browser wants to communicate, but the connection is not yet established. Many servers in use today can handle only a finite number of these half-way completed con-

nections at a time. They are stored in a backlog until they are completed or time out. When the server's backlog is full, no new connections can be accepted.

A SYN Flood attack attempts to fill up the victim server's backlog by sending a flood of SYN segments without ever sending an ACK. When the backlog fills up, the server will be unavailable to users.

WatchGuard System Manager can help defend your servers against a SYN Flood attack by tracking the number of SYNs that are sent without a following ACK. If this number exceeds the threshold you define, the SYN Flood protection feature will self-activate. Once active, further connection attempts from the external side of the Firebox must be verified before being allowed to reach your servers. Connections that cannot be verified are not allowed through, thus protecting your server from having a full backlog.

The SYN Flood protection feature will self-deactivate when it senses the attack is over.

From Policy Manager:

1 On the toolbar, click the Default Packet Handling icon.
You can also, from Policy Manager, select Setup ⇒ Intrusion Prevention ⇒ Default Packet Handling.
The Default Packet Handling dialog box appears.

2 Select the checkbox marked **Block SYN Flood Attacks**.

Changing SYN flood settings

Active SYN flood defenses can occasionally prevent legitimate connection attempts from being completed. If you find that too many legitimate connection attempts fail when your SYN flood defense is active, you can change SYN flood settings to minimize this problem.

You can set the maximum number of incomplete TCP connections the Firebox allows before the SYN flood defense is activated. The default setting of 60 means that when the number of TCP connections waiting to be validated climbs to 61 or above, SYN flood defense is activated. Conversely, when the number of connections waiting for validation drops to 59 or less, SYN flood defense is deactivated. You might need to adjust this setting to custom-fit the SYN Flood protection feature for

your network. Every time the feature self-activates, a log message will be recorded stating `SYN Validation: activated`. When the feature self-deactivates, the log message `SYN Validation: deactivated` will be recorded. If these messages occur frequently when your server is not under attack, the Maximum Incomplete Connections setting may be too low. If the SYN Flood protection feature is not preventing attacks from affecting your server, the setting may be too high. Consult your server's documentation for help choosing a new value, or experiment by adjusting the setting until the problems disappear.

The validation timeout controls how long the Firebox "remembers" clients that pass the validation test. The default setting of 120 seconds means that a client that drops a legitimate connection has a two-minute window to reconnect without being challenged. Setting the validation timeout to zero seconds means that legitimate connections are "forgotten" when dropped, so every connection attempt is challenged.

From Policy Manager:

1 On the toolbar, click the Default Packet Handling icon.
You can also, from Policy Manager, select Setup ⇒ Intrusion Prevention ⇒ Default Packet Handling.
The Default Packet Handling dialog box appears.

2 Use the **SYN Validation Timeout** box to set how long the Firebox "remembers" a validated connection after that connection is dropped.

3 Use the **Maximum Incomplete Connections** box to set the number of connections awaiting validation that are allowed to queue before the Firebox automatically activates SYN flood defense.

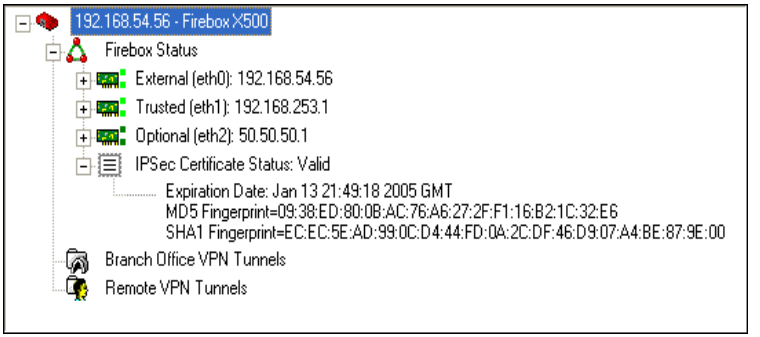
Detecting Man-in-the-Middle Attacks

Man-in-the-middle attacks deceive two parties into thinking they are communicating with each other while they are actually both communicating with a third party. The attacker can then intercept data passing through the connection.

To detect whether a man-in-the-middle attack is in progress:

1 Bring up the user interface for the Certificate Authority.
The browser displays the fingerprint for the CA certificate.

2 Verify the certificate against the one displayed in Firebox System Manager, **Front Panel** tab, as shown in the following figure.



Blocking Sites

The Blocked Sites feature of the Firebox helps you prevent unwanted contact from known or suspected hostile systems. After you identify an intruder, you can block all attempted connections from them. You can also configure logging to record all access attempts from these sources so you can collect clues as to what services they are attempting to attack.

A blocked site is an IP address outside the Firebox that is prevented from connecting to hosts behind the Firebox. If any packet comes from a host that is blocked, it does not get past the Firebox.

There are two kinds of blocked sites:

- Permanently blocked sites—which are listed in the configuration file and change only if you manually change them.
- Auto-blocked sites—which are sites the Firebox adds or deletes dynamically based on default packet handling rules and service-by-service rules for denied packets. For

example, you can configure the Firebox to block sites that attempt to connect to forbidden ports. Sites are temporarily blocked until the auto-blocking mechanism times out.

For information on auto-blocking sites using the protocol anomaly detection (PAD) feature, see "Configuring the Incoming SMTP Proxy" on page 128.

WatchGuard System Manager auto-blocking and logging mechanisms can help you decide which sites to block. For example, when you find a site that spoofs your network, you can add the offending site's IP address to the list of permanently blocked sites.

Note that site blocking can be imposed only to traffic on the Firebox's external interface.

Blocking a site permanently

You may know of hosts on the Internet that pose constant dangers, such as a university computer that has been used more than once by student hackers who try to invade your network.

Use Policy Manager to block a site permanently. The default configuration blocks three network addresses—10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. These are the private ("unconnected") network addresses. Because they are for private use, backbone routers should never pass traffic with these addresses in the source or destination field of an IP packet. Traffic from one of these addresses is almost certainly a spoofed or otherwise suspect address. RFCs 1918, 1627, and 1597 cover the use of these addresses.

NOTE

The Blocked Sites list applies only to traffic on the External interface.

From Policy Manager:

1 On the toolbar, click the Blocked Sites icon (shown at right).



You can also select Setup ⇒ Intrusion Prevention ⇒ Blocked Sites. The Blocked Sites dialog box appears, as shown in the following figure.

2 Click **Add**.

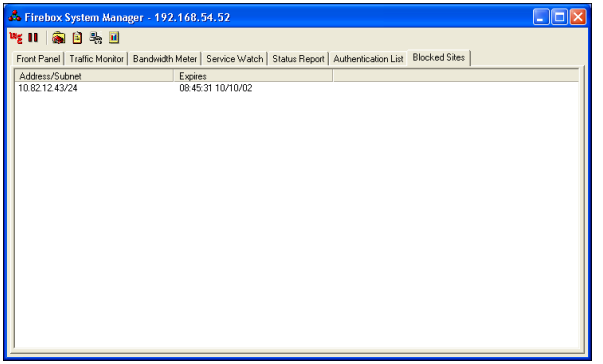
3 Use the **Choose Type** drop list to select a member type. The options are **Host IP Address**, **Network IP Address**, or **Host Range**.

4 Enter the member value.

Depending on the member type, this can be an IP address or a range of IP addresses. When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

5 Click **OK**.

The Blocked Sites dialog box appears displaying the new site in the Blocked Sites list.



Using an external list of blocked sites

You can create a list of blocked sites in an external file. This file must be a `.txt` file. To load an external file into your blocked sites list:

1 In the **Blocked Sites** dialog box, click **Import**.

2 Browse to locate the file. Double-click it, or select it and click **Open**.

The contents of the file are loaded into the Blocked Sites list.

Creating exceptions to the Blocked Sites list

A blocked site exception is a host that is not added to the list of automatically blocked sites regardless of whether it fulfills criteria that would otherwise add it to the list. The site can still be blocked according to the Firebox configuration, but it will not be automatically blocked for any reason.

From Policy Manager:

1 Select **Setup** ⇒ **Intrusion Prevention** ⇒ **Blocked Sites Exceptions**.
The Blocked Sites Exceptions dialog box appears.

2 Click **Add**.

3 Enter the IP address of the site for which you want to create an exception. Click **OK**.

4 Click **OK** to close the **Blocked Sites Exceptions** dialog box.

To remove an exception, select the IP address of the site to remove. Click **Remove**.

Changing the auto-block duration

From the **Blocked Sites** dialog box, either type or use the scroll control to change the duration, in minutes, that the firewall automatically blocks suspect sites. Duration can range from 1 to 32,000 minutes (about 22 days).

Logging and notification for blocked sites

From the **Blocked Sites** dialog box:

1 Click **Logging**.
The Logging and Notification dialog box appears.

2 In the **Category** list, click **Blocked Sites**.

3 Modify the logging and notification parameters according to your security policy preferences.
For detailed instructions, see "Customizing Logging and Notification by Service or Option" on page 197.

Blocking Ports

You can block ports to explicitly disable external network services from accessing ports that are vulnerable as entry points to your network. A blocked port setting takes precedence over any of the individual service configuration settings.

Like the Blocked Sites feature, the Blocked Ports feature blocks only packets that enter your network through the external interface.

You should consider blocking ports for several reasons:

- Blocked ports provide an independent check for protecting your most sensitive services, even when another part of the firewall is not configured correctly.
- Probes made against particularly sensitive services can be logged independently.
- Some TCP/IP services that use port numbers above 1024 are vulnerable to attack if the attacker originates the connection from an allowed well-known service with a port number below 1024. These connections can be attacked by appearing to be an allowed connection in the opposite direction. You can prevent this type of attack by blocking the port numbers of services whose port numbers are under 1024.

By default, the Firebox blocks several destination ports. This measure provides convenient defaults which do not normally require changing. Typically, the following services should be blocked:

X Window System (ports 6000-6063)

The X Window System (or X-Windows) has several distinct security problems that make it a liability on the Internet. Although several authentication schemes are available at the X server level, the most common ones are easily defeated by a knowledgeable attacker. If an attacker can connect to an X server, he or she can easily record all keystrokes typed at the workstation, collecting passwords and other sensitive information. Worse, such intrusions can be difficult or impossible to detect by all but the most knowledgeable users.

The first X Window server is always on port 6000. If you have an X server with multiple displays, each new display uses an additional port number after 6000, up to 6063 for a maximum of 64 displays on a given host.

X Font Server (port 7100)

Many versions of X-Windows support font servers. Font servers are complex programs that run as the super-user on some hosts. As such, it is best to explicitly disable access to X font servers.

NFS (port 2049)
NFS (Network File System) is a popular TCP/IP service for providing shared file systems over a network. However, current versions have serious authentication and security problems which make providing NFS service over the Internet very dangerous.

NOTE

Port 2049 is not assigned to NFS; however, in practice, this is the most common port used for NFS. The port assigned for NFS is assigned by the portmapper. If you're using NFS, it would be a good idea to verify that NFS is using port 2049 on all your systems.

OpenWindows (port 2000)
OpenWindows is a windowing system from Sun Microsystems that has similar security risks to X-Windows.

rlogin, rsh, rcp (ports 513, 514)
These services provide remote access to other computers and are somewhat insecure on the Internet. Because many attackers probe for these services, it is a good idea to block them.

RPC portmapper (port 111)
RPC Services use port 111 to determine which ports are actually used by a given RPC server. Because RPC services themselves are very vulnerable to attack over the Internet, the first step in attacking RPC services is to contact the portmapper to find out which services are available.

port 0
Port 0 is reserved by IANA, but many programs that scan ports start their search on port 0.

port 1
Port 1 is for the rarely used TCPmux service. Blocking it is another way to confuse port scanning programs.

Novell IPX over IP (port 213).
If you use Novell IPX over IP internally, you might want to explicitly block port 213.

NetBIOS services (ports 137 through 139)
You should block these ports if you use NetBIOS internally. Although such services are blocked implicitly by default packet handling, blocking them here provides additional security.

Avoiding problems with legitimate users

It is possible for legitimate users to have problems because of blocked ports. In particular, some clients might temporarily fail because of blocked ports.

You should be very careful about blocking port numbers between 1000 through 1999, as these numbers are particularly likely to be used as client ports.

NOTE

Solaris uses ports greater than 32768 for clients.

Blocking a port permanently

From Policy Manager:

1 On the toolbar, click the Blocked Ports icon, shown at right.

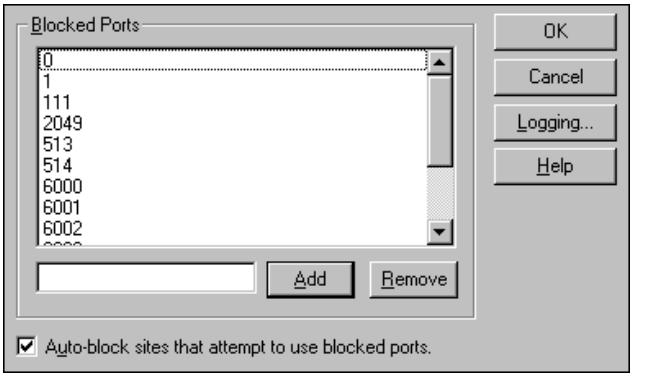


You can also select Setup ⇒ Intrusion Prevention ⇒ Blocked Ports. The Blocked Ports dialog box appears, as shown in the following figure.

2 In the text box to the left of the **Add** button, type the port number. Click **Add**.

The new port number appears in the Blocked Ports list.

To remove a blocked port, select the port to remove. Click **Remove**.



Auto-blocking sites that try to use blocked ports

You can configure the Firebox such that when an outside host attempts to access a blocked port, that host is temporarily auto-blocked.

In the **Blocked Ports** dialog box, select the checkbox marked **Auto-block sites that attempt to use blocked ports**.

You can also auto-block sites using protocol anomaly detection. For more information, see "Configuring the Incoming SMTP Proxy" on page 128.

Setting logging and notification for blocked ports

You can also adjust your event logs and notification to accommodate attempts to access blocked ports. You can configure the Firebox to log all attempts to use blocked ports, or notify a network administrator when someone attempts to access a blocked port.

From the **Blocked Ports** dialog box:

1 Click **Logging**.
The Logging and Notification dialog box appears.

2 In the **Category** list, click **Blocked Ports**.

3 Modify the logging and notification parameters according to your security policy preferences.
For detailed instructions, see "Customizing Logging and Notification by Service or Option" on page 197.

Blocking Sites Temporarily with Service Settings

Use service properties to automatically and temporarily block sites when incoming traffic attempts to use a denied service. You can use this feature to individually log, block, and monitor sites that attempt access to restricted ports on your network.

Configuring a service to temporarily block sites

Configure the service to automatically block sites that attempt to connect using a denied service. From Policy Manager:

1. Double-click the service icon in the Services Arena.
   The Properties dialog box appears.
2. Use the **Incoming service Connections Are** drop-down list to select **Enabled and Denied**.
3. Select the checkbox marked **Auto-block sites that attempt to connect via** *service*, located at the bottom of the dialog box.

Viewing the Blocked Sites list



The Blocked Sites list is a compilation of all sites currently blocked by the Firebox. Use Firebox Monitors to view sites that are automatically blocked according to a service's property configuration. From System Manager, click the **Blocked Site List** tab at the bottom of the graph. (You might need to use the arrows to access this tab.)

Integrating Intrusion Detection

Intrusion detection is an important component of a defense-in-depth security policy. A good intrusion detection system (IDS) examines over time the source, destination, and type of traffic directed at your network and compares it against known patterns of attack. When a match occurs, it tells you the nature of the attack and recommends possible courses of action.

WatchGuard System Manager default packet handling options provide a basic intrusion detection system by blocking common and readily recognizable attacks such as IP address spoofing and linear port space probes. The intrusion detection capabilities of the Firebox, however, are necessarily limited. The primary func-

tion of your firewall is to examine and either allow or deny packets. Little extra bandwidth is available to conduct sophisticated analysis of traffic patterns.

LiveSecurity Service subscribers can download a command-line utility called the Firebox System Intrusion Detection System Mate (fbidsmate) that integrates the Firebox with most commercial and shareware IDS applications. You use the fbidsmate utility to configure your IDS to run scripts that query the Firebox for information. Because versions are available for Win32 (Windows NT, Windows 2000, and Windows XP), SunOS, and Linux operating systems, you can select whatever IDS application best suits your security policy and network environments.

Working with an external IDS application, the Firebox can automatically add sites to the Blocked Sites list. Timeouts and blocked site exceptions work exactly as they do for sites blocked using default packet handling options. Sites added to the Blocked Sites list appear in the Firebox Monitors **Blocked Sites** tab. In addition, you can use the utility to add explanatory log messages to the log file which can subsequently be used for reports.

Because the fbidsmate utility is external to the Firebox, no changes in the configuration file are required, nor is there anything additional to configure using Policy Manager.

To obtain a copy of the fbidsmate command-line utility that matches the operating system on which your IDS application is running, log in to your LiveSecurity Service account at:
https://www.watchguard.com/support

Using the fbidsmate command-line utility

The fbidsmate utility works from the command line. Although you can execute the commands directly against the Firebox, the tool is used most frequently in the context of an IDS application script. The command syntax is:

fbidsmate firebox_address [rwpassphrase | -f rwpassphrase_file] [add_hostile hostile_address] | [add_log_message priority(0-7) "message"]

fbidsmate import_passphrase rwpassphrase rwpassphrase_filename

add_hostile
This command adds a site to the Auto-Blocked Site list, with the duration set by the administrator in Policy Manager's **Blocked Sites** dialog box. It effectively extends your control of the Auto-Block mechanism inside the Firebox.

add_log_message
This command causes a message to be added to the log stream emitted by the Firebox. Because the priority is used by the Firebox to construct syslog messages, its range is the standard syslog 0=Emergency to 7=Debug. There is no limit on message length; the message is automatically broken into multiple messages if necessary.

import_passphrase
You can store the Firebox configuration passphrase in encrypted form instead of putting it in clear text in your IDS scripts. This command stores the passphrase in the designated file using 3DES encryption. Rather than using the configuration passphrase, use the file name in your scripts. If you are managing multiple Fireboxes, you need one passphrase file per Firebox.

Return value

The return value of fbidsmate is zero if the command executed successfully; otherwise it is non-zero. This value should be checked upon return if calling fbidsmate from a shell script or through some other interface.

Examples

In the following examples, the IP address of the Firebox is 10.0.0.1 with a configuration passphrase of "secure1".

Example 1
The IDS detects a port scan from 209.54.94.99 and asks the Firebox to block that site:

```
fbidsmate 10.0.0.1 secure1 add_hostile
209.54.94.99
```

The 209.54.94.99 site appears on the auto-blocked sites list and remains there for the duration set in Policy Manager. In addition, the following message appears in the log file:

```
Temporarily blocking host 209.54.94.99
```

Example 2

The IDS adds a message to the Firebox's log stream:

```
fbidsmate 10.0.0.1 secure1 add_log_message
3 "IDS system temp. blocked 209.54.94.99"
```

With the IDS running on host 10.0.0.2, the following message appears in the Firebox log file:

```
msg from 10.0.0.2: IDS system temp. blocked
209.54.94.99
```

Example 3

Because you are running your IDS application outside the firewall perimeter, you decide to encrypt the configuration passphrase used in your IDS scripts. Note that even with encryption, you should lock down the IDS host as tightly as possible. First, you must import the passphrase "secure1" to an encrypted file on the IDS host:

```
fbidsmate import_passphrase secure1 /etc/
fbidsmate.passphrase
Then you could rewrite the previous examples as:
fbidsmate 10.0.0.1 -f /etc/fbidsmate.passphrase
add_hostile 209.54.94.99
fbidsmate 10.0.0.1 -f /etc/fbidsmate.passphrase
add_log_message 3 "IDS system temp. blocked
209.54.94.99"
```

CHAPTER 12

Setting Up Logging and Notification

An *event* is any single activity that occurs at the Firebox, such as denying a packet from passing through the Firebox. *Logging* is the recording of these events to a log host. A *notification* is a message sent to the administrator by the Firebox when an event occurs that indicates a security threat. Notification can be in the form of email, a popup window on the WatchGuard Security Event Processor (WSEP), a call to a pager, or the execution of a custom program.

For example, WatchGuard recommends that you configure default packet handling to issue a notification when the Firebox detects a port space probe. When the Firebox detects one, the log host sends notification to the network security administrator about the rejected packets. At this point, the network security administrator can examine the logs and decide what to do to further secure the organization's network. Some possible courses of action would be to:

- Block the ports on which the probe was attempted
- Block the IP address that is sending the packets
- Contact the ISP through which the packets are being sent

Logging and notification are crucial to an effective network security policy. Together, they make it possible to monitor your network security, identify both attacks and attackers, and take

action to address security threats and challenges. WatchGuard logging and notification features are both flexible and powerful. You can configure your firewall to log and notify a wide variety of events, including specific events that occur at the level of individual services. For more information on logging, see the following collection of FAQs:
https://www.watchguard.com/support/advancedfaqs/log_main.asp

Developing Logging and Notification Policies

When creating a logging policy, you spell out what gets logged and when an event or series of events warrants sending out a notification to the on-duty administrator. Developing these policies simplifies the setup of individual services in WatchGuard System Manager. If you have fully mapped out a policy, you can more easily delegate configuration duties and ensure that individual efforts do not contradict the overall security stance or logging and notification policies.

Logging policy

Specifically, the logging policy delineates:

- Which events to log
- Which service events to log
- Which servers are allocated as log hosts
- How large a log file is allowed to become and how often a new log file is created

In general, you want to log only the events that might indicate a potential security threat, and ignore events that would waste bandwidth and server storage space. This generally translates into logging spoofs, IP options, probes, and denied packets, and not logging allowed packets. Allowed packets should not be indicative of a security threat. Furthermore, allowed traffic usually far exceeds the volume of denied traffic and would slow response times as well as causing the log file to grow and turn over too quickly.

WatchGuard provides the option to log allowed events primarily for diagnostic purposes when setting up or troubleshooting an installation. Or, you might have a situation such as a very spe-

cialized service that uses an obscure, very high port number, and the service is intended for use only by a small number of people in an organization. In that case you might want to log all traffic for that service so you can monitor or review that service activity.

Not all denied events need to be logged. For example, if incoming FTP denies all incoming traffic from any source outside to any destination inside, there is little point in logging incoming denied packets. All traffic for that service in that direction is blocked.

Notification policy

The most important events that should trigger notification are IP options, port space probes, address space probes, and spoofing attacks. These are configurable in the **Default Packet Handling** dialog box, described in "Default Packet Handling" on page 165.

Other notifications depend on your Firebox configuration and how much time is available for interacting with it. For example, if you set up a simple configuration that enables only a few services and denies most or all incoming traffic, only a few circumstances warrant notification. On the other hand, if you have a large configuration with many services; with many allowed hosts or networks for incoming traffic; popular protocols to specific, obscure ports; and several filtered services added of your own design; you will need to set up a large, complex notification scheme. This type of configuration is more vulnerable to attack. Not only are there many more services that require a notification policy, the high number of routes through the Firebox increases the likelihood that the log host will issue frequent notifications. If you set up a very accommodating firewall, be prepared to spend a large amount of time interacting with your security system or fixing security breaches.

To formulate a notification policy, look at the number and nature of the services enabled for the Firebox, and how open or limited each service is. In general, for the high-traffic proxies such as SMTP and FTP, you might activate a repeat notification if the service rejects five to ten packets within 30 seconds. If you have set up a specialized service limited to traffic between two

or three hosts using a high port number, you might want to activate notification on this service whenever it denies *or* passes a packet.

Failover Logging

WatchGuard uses failover logging to minimize the possibility of missing log events. With failover logging, you configure a list of log hosts to accept logs in the event of a failure of the primary log host. By default, the Firebox sends log messages to the primary log host. If for any reason the Firebox cannot establish communication with the primary log host, it automatically sends log messages to the second log host. It continues through the list until it finds a log host capable of recording events.

Multiple log hosts operate in failover mode, not redundancy mode—that is, events are not logged to multiple log hosts simultaneously; they are logged only to the primary log host unless that host becomes unavailable. The logs are then passed on to the next available log host according to the order of priority.

Except where Syslog is used, the WatchGuard Security Event Processor software must be installed on each log host. For more information, see "Setting up the WatchGuard Security Event Processor" on page 190.

WatchGuard Logging Architecture

By default, Policy Manager and the log and notification application—the WatchGuard Security Event Processor—are installed on the same computer. You can, however, install the event processor software on multiple computers.

You must complete the following tasks to configure the firewall for logging and notification:

Policy Manager

- Add log hosts
- Customize preferences for services and packet handling options

- Save the configuration file with logging properties to the Firebox

WatchGuard Security Event Processor (WSEP)

- Install the WSEP software on each log host
- Set global logging and notification preferences for the host
- Set the log encryption key on each log host identical to the key set in Policy Manager

Designating Log Hosts for a Firebox

You should have at least one log host to run WatchGuard System Manager. The default primary log host is the management station that is set when you run the QuickSetup Wizard. You can specify a different primary log host as well as multiple backup log hosts. The typical medium-sized operation has two or three high-capacity log hosts.

Multiple log hosts operate in failover, not redundant mode. The primary log host handles the bulk of the logging duties; others are called in as needed when the highest-ranking log host is unavailable to receive logs.

Before setting up a log host, you need to have the following information:

- IP address of each log host
- Encryption key to secure the connection between the Firebox and log hosts
- Priority order of primary and backup log hosts

For log host troubleshooting information, see the following FAQ:
https://www.watchguard.com/support/advancedfaqs/log_troubleshootinghost.asp

Adding a log host

From Policy Manager:

1 Select **Setup ⇒ Logging**.
The Logging Setup dialog box appears.

2 Click **Add**.

The Add IP Address dialog box appears, as shown in the following figure.



3 Enter the IP address to be used by the log host.

When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

4 Enter the encryption key that secures the connection between the Firebox and the log host.

The default encryption key is the status passphrase set in the QuickSetup Wizard. You must use the same log encryption key for both the Firebox and the WatchGuard Security Event Processor.

5 Click **OK**.

Repeat until all primary and backup log hosts appear in the WatchGuard Security Event Processors list.

Enabling Syslog logging

Note that Syslog logging is not encrypted; therefore, do not set the Syslog server to a host on the external interface. From Policy Manager:

1 Select **Setup** ⇒ **Logging**.

The Logging Setup dialog box appears.

2 Click the **Syslog** tab.

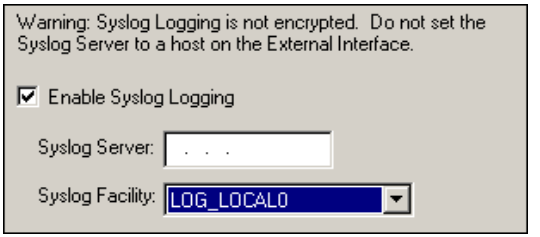
The Syslog tab information appears as shown in the following figure.

3 Select the checkbox marked **Enable Syslog Logging**.

4 Enter the IP address of the Syslog server.

5 Select a Syslog facility from the drop-down list. You can select a facility from LOG_LOCAL_0 through LOG_LOCAL_7.

6 Click **OK**.


Warning: Syslog Logging is not encrypted. Do not set the Syslog Server to a host on the External Interface.
Enable Syslog Logging
Syslog Server:
Syslog Facility:
LOG_LOCAL0

For more information on Syslog logging, see the following FAQ: https://www.watchguard.com/support/advancedfaqs/log_syslog.asp

Changing the log encryption key

Edit a log host entry to change the log encryption key. From Policy Manager:

1 Select **Setup** ⇒ **Logging**.
The Logging Setup dialog box appears.

2 Click the host name. Click **Edit**.

3 Type in the new log encryption key. Click **OK**.
You must use the same log encryption key for both the Firebox and the WatchGuard Security Event Processor. To change the log encryption key on the WSEP application, see "Setting the log encryption key" on page 193.

Removing a log host

Remove a log host when you no longer want to use it for any logging purpose. From Policy Manager:

1 Select **Setup** ⇒ **Logging**.
The Logging Setup dialog box appears.

2 Click the host name. Click **Remove**.

3 Click **OK**.
The Logging Setup dialog box closes and removes the log host entry from the configuration file.

Reordering log hosts

Log host priority is determined by the order in which the hosts appear in the WatchGuard Security Event Processor list. The host that is listed first receives log messages.

Use the **Up** and **Down** buttons to change the order of the log hosts. From the **Logging Setup** dialog box:

- To move a host down, click the host name. Click **Down**.
- To move a host up, click the host name. Click **Up**.

Synchronizing log hosts

Synchronizing log hosts involves setting the clocks of all your log hosts to a single common time source. This keeps logs orderly and prevents time discrepancies in the log file if failovers occur.

The Firebox sets its clock to the current log host. If the Firebox and the log host times are different, the Firebox time drifts toward the new time, which often results in a brief interruption in the log file. Rebooting the Firebox resets the Firebox time to that of the primary log host. Therefore, you should set all log hosts' clocks to a single source. In a local installation where all log hosts are on the same domain, set each log host to the common domain controller.

For Windows NT log hosts

1 Go to each log host. Open an MS-DOS Command Prompt window. Type the following command:

`net time /domain:domainName /set`

where *domainName* is the domain in which the log hosts operate.

The system returns a message naming the domain controller.

2 Type `Y`.

The time of the local host is set to that of the domain controller.

Another method to set the log host (and domain controller) clocks is to use an independent source such as the atomic clock–based servers available on the Internet. One place to access this service is:
http://www.bldrdoc.gov/timefreq

Setting up the WatchGuard Security Event Processor

The WatchGuard Security Event Processor application is available both as a command-line utility and, on a Windows NT, Windows 2000, or Windows XP host, as a service. It is, by default, installed on the management station when you install

WatchGuard System Manager. However, you must manually install the WSEP on all log hosts.

Running the WSEP application on Windows NT, Windows 2000, or Windows XP

If the WSEP application is to run on a Windows NT, 2000, or XP operating system, you can choose between two methods: interactive mode from a DOS window or as a Windows service. The default method is for the WSEP application to run as a Windows service.

By default, the WSEP application is installed to run as a Windows service, starting automatically every time the host computer restarts.

1 To start the WatchGuard Security Event Processor service:
   - In Windows NT, go to **Start ⇒ Settings ⇒ Control Panel ⇒ Services.**
   - In Windows 2000, go to **Start ⇒ Settings ⇒ Control Panel ⇒ Administrative Tools ⇒ Services**.
   - In Windows XP, go to **Start ⇒ Control Panel ⇒ Administrative Tools ⇒ Services**.

2 Double-click or right-click **WG Security Event Processor**. Click **Start**.
   - Or, right-click on the WSEP icon in the system tray and select **Start**.
   - You can also restart your computer. The service starts automatically every time the host reboots.

In addition, if the WSEP application is running as a service and you are using pop-up notifications, make sure the service can interact with the Desktop.

1 Verify that the WatchGuard Security Event Processor service is enabled to interact with the desktop:
   - In Windows NT, go to **Start ⇒ Settings ⇒ Control Panel ⇒ Services.**
   - In Windows 2000, go to **Start ⇒ Settings ⇒ Control Panel ⇒ Administrative Tools ⇒ Services**.
   - In Windows XP, go to **Start ⇒ Control Panel ⇒ Administrative Tools ⇒ Services**.

2 Double-click **WG Security Event Processor**. Click the **Log On** tab.

3 Verify that the **Allow service to interact with desktop** checkbox is selected.

4 If the WSEP application was running, restart it *after* saving the changes.

As a service, using the Command Prompt

If the WSEP application was not installed by the WatchGuard System Manager installation wizard, this must be done from the Command Prompt DOS window.

1 Select **Start** ⇒ **Run** and type: `command`.
A Command prompt window appears.

2 Change directories to the WatchGuard installation directory.
The default installation directory is C:\Program Files\WatchGuard.

3 At the command line, type:
`controld -nt-install`

You can perform other commands for the WSEP application from the Command Prompt:

- To start the WSEP application, at the command line, type:
  `- controld -nt-start`
- To stop the WSEP application, at the command line, type:
  `- controld -nt-stop`
- To remove the WSEP application, at the command line, type:
  `- controld -nt-remove`

Interactive mode from a Command Prompt

The WSEP application can also run in interactive mode from a Command Prompt window. To so this, type: `controld –NT –interactive`

NOTE

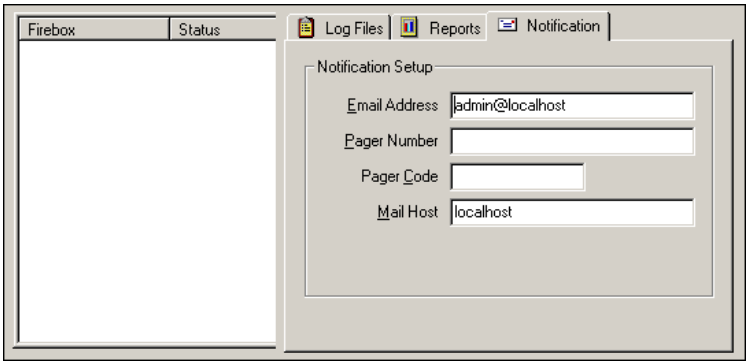
You can minimize the Command Prompt window. However, do *not* close it. Closing the Command Prompt window halts the WSEP application.

Viewing the WSEP application



While the WatchGuard Security Event Processor is running, a Firebox-and-traffic icon (shown at left) appears in the Windows Desktop tray. To view the WSEP application, right-click the tray icon and select **WSEP Status/Configuration**. The status and configuration information appears as shown in the following figure.

If the WatchGuard Security Event Processor icon is not in the tray, in Firebox System Manager, select **Tools ⇒ Logging ⇒ Event Processor Interface**. To start the Event Processor interface when you log in to the system, add a shortcut to the **Startup** folder in the **Start** menu. The WatchGuard installation program does this automatically if you set up logging.



Starting and stopping the WSEP

The WSEP starts automatically when you start the host on which it resides. However, it is possible to stop or restart the WSEP from its interface at any time. Open the WatchGuard Security Event Processor interface:

- To start the WSEP application, select **File ⇒ Start Service**.
- To stop the WSEP application, select **File ⇒ Stop Service**.

Setting the log encryption key

The log connection (but not the log file) between the Firebox and a log host is encrypted for security purposes. Both the man-

agement station and the WSEP application must have the same encryption key.

NOTE

You must enter an encryption key for the log host to receive logs from the Firebox. It must be the same key used when adding a WSEP application to the management station.

From the WatchGuard Security Event Processor user interface:

1 Select **File ⇒ Set Log Encryption Key.**

2 Enter the log encryption key in both text boxes. Click **OK.**

Setting Global Logging and Notification Preferences

The WatchGuard Security Event Processor lists the connected Firebox and displays its status. It has three control areas, which are used as follows:

Log Files tab
Specify the maximum number of records stored in the log file.

Reports tab
Schedule regular reports of log activity.

Notification tab
Control to whom and how notification takes place.

Together, these controls set the general parameters for most global event processing and notification properties.

Log file size and rollover frequency

You can set the maximum size of the log file by number of log entries or by time (such as daily, weekly, or monthly). When the log file reaches the maximum according to your settings, the log host creates a new file or overwrites the old file. Log rollover is the frequency at which log files begin overwriting.

For example, suppose you have set your log file maximum to 100,000 entries. Operation of your Firebox begins on July 21. By July 26, the log file has 100,000 entries. At this point, the log host starts writing July 27 log entries to a new file and the other file becomes the old file.

The ideal maximum log file size is highly individual: It will be based on the storage space available, how many days of log entries you want on hand at any time, and how long a log file is practical to keep, open, and view. How quickly a file hits its maximum size and is overwritten is also determined by how many event types are logged and how much traffic the Firebox processes. For example, a small operation might not see 10,000 entries in two weeks, whereas a large one with many services enabled might easily log 100,000 entries in a day.

When considering your ideal maximum log file, consider how often you plan to issue reports of the Firebox activity. WatchGuard Historical Reports uses a log file as its source to build reports. If you issue weekly reports to management, you would want a log file large enough to hold a typical eight or nine days' worth of events. Watch your initial log file configuration to see how many days' events it collects before turning over, and then adjust the size to your reporting needs.

Setting the interval for log rollover

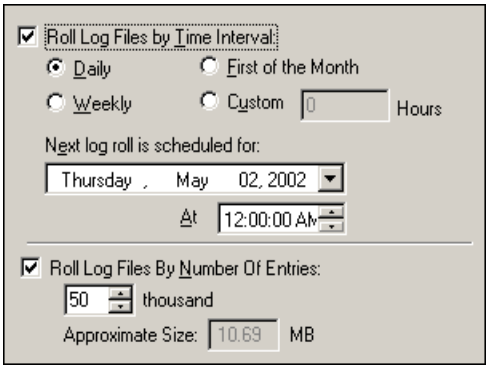
You can control when the WSEP application rolls over using the **Log Files** tab in the WatchGuard Security Event Processor. The WSEP application can be configured to roll over by time interval, number of entries, or both. From the WatchGuard Security Event Processor interface:

1 Click the **Log Files** tab.
The Log Files tab information appears, as shown in the following figure.

2 For a time interval, select the **Roll Log Files By Time Interval** checkbox. Select the frequency. Use the **Next Log Roll is Scheduled For** drop-down list to select a date. Use the scroll control or enter the first time of day.

3 For a record size, select the **Roll Log Files By Number of Entries** checkbox. Use the scroll control or enter a number of log record entries.
The Approximate Size field changes to display the approximate file size of the final log file. For a detailed description of each control, right-click it, and then select What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

4 Click **OK**.
The WSEP interface closes and saves your entries. New settings take effect immediately.



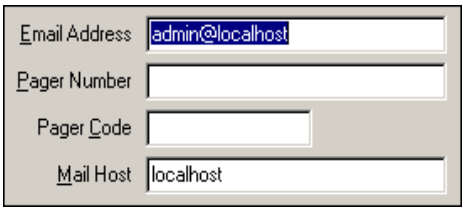
Scheduling log reports

You can use the WSEP application to schedule the automatic generation of network activity reports. For more information, see “Scheduling a report” on page 224.

Controlling notification

Notification occurs when the Firebox sends an email message, pops up a window on the log host, dials a pager, or executes a program to notify an administrator that the Firebox has detected a triggering event. Use the WSEP application to control when and to whom such notifications are sent. From the WatchGuard Security Event Processor interface:

1 Click the **Notification** tab.
The Notification tab information appears, as shown in the following figure.



2 Modify the settings according to your security policy preferences.

For more information on individual settings, right-click the setting, and then select What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

Setting a Firebox friendly name for log files

You can give the Firebox a friendly name to be used in log files. If you do not specify a name, the Firebox's IP address is used. From Policy Manager:

1 Select **Setup ⇒ Name**.

The Firebox Name dialog box appears.

2 Enter the friendly name of the Firebox. Click **OK**.

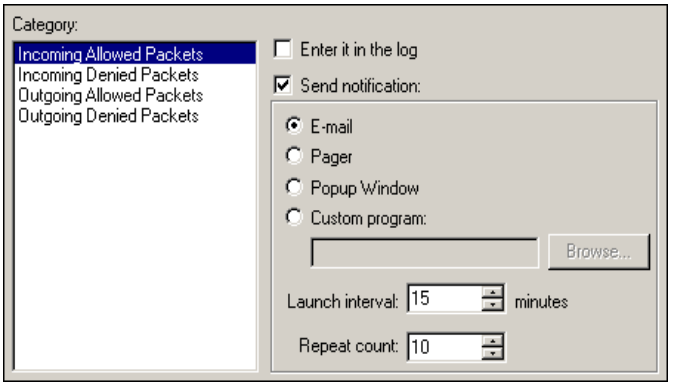
All characters are allowed except blank spaces and forward or back slashes (/ or \).

For more information on the log file names used by WatchGuard System Manager, see the following FAQ:
https://www.watchguard.com/support/advancedfaqs/log_filename.asp

Customizing Logging and Notification by Service or Option

WatchGuard System Manager allows you to create custom logging and notification properties for each service and blocking option. You can fine-tune your security policy, logging only those events that require your attention and limiting notification to those of truly high priority.

To make logging and notification configuration easier, services, blocking categories, and packet-handling options share an identical dialog box, as shown in the following figure. Therefore, once you learn the controls for one type of service, you can easily configure the remainder.



You can define the following:

Category
The event types that can be logged by the service or option. This list changes depending on the service or option. Click the event name to display and set its properties.

Enter it in the log
Select this checkbox to log the event type; clear it to disable logging for the event type. Because the Firebox must perform domain name resolution, there may be a time lag before logs appear in the log file. All denied packets are logged by default.

Send Notification
Select this checkbox to enable notification for the event type; clear it to disable notification for the event type.

The remaining controls are active when you select the **Send Notification** checkbox:

Email
Sends an email message when the event occurs. Set the email recipient in the **Notification** tab of the WSEP user interface.

Pager
Triggers an electronic page when the event occurs. Set the pager number in the **Notification** tab of the WSEP user interface.
If the pager is accessible by email, select the **Email** option, and then enter the email address of the pager in the **Notification** tab of the WSEP user interface.

Popup Window
Makes a pop-up window appear on the log host when the event occurs.

Custom Program
Triggers execution of a custom program when the event occurs. A custom batch file or program enables you to trigger multiple types of notification. Type the full path to the program in the accompanying field, or use **Browse** to locate and select the program.

NOTE
WatchGuard allows only one notification type per event.

Setting Launch Interval and Repeat Count

Two parameters work in conjunction with the Event Processor Repeat Interval to control notification timing:

Launch Interval
The minimum time (in minutes) between separate launches of a notifier. Set this parameter to prevent the launch of several notifiers in response to similar events that take place in a short amount of time.

Repeat Count
The threshold for how often an event can repeat before the Firebox activates the special repeat notifier. The repeat notifier creates a log entry stating that the notifier in question is repeating. Notification repeats only after this number of events occurs.

As an example of how these two values interact, suppose you have set up notification with these values:

- Launch interval = 5 minutes
- Repeat count = 4

A port space probe begins at 10:00 a.m. and continues once per minute, triggering the logging and notification mechanisms. Here is the time line of activities that would result from this event with the above timing and repeating setup:

1 10:00—Initial port space probe (first event)

2 10:01—First notification launched (one event)

3 10:06—Second notification launched (reports five events)

4 10:11—Third notification launched (reports five events)

5 10:16—Fourth notification launched (reports five events)

The time intervals between activities 1, 2, 3, 4, and 5 are controlled by the launch interval, which was set to 5 minutes.

The repeat count multiplied by the launch interval equals the amount of time an event must continuously happen before it is handled as a repeat notifier.

Setting logging and notification for a service

For each service added to the Services Arena, you can control logging and notification of the following events:

- Incoming packets that are allowed
- Incoming packets that are denied
- Outgoing packets that are allowed
- Outgoing packets that are denied

From Policy Manager:

1 Double-click a service in the Services Arena.
The Properties dialog box appears.

2 Click **Logging**.
The Logging and Notification dialog box appears. The options for each service are identical; the main difference is based on whether the service in question is for incoming, outgoing, or bidirectional communication.

3 Modify logging and notification properties according to your security policy preferences. Click **OK**.

Setting logging and notification for default packet-handling options

When this option is selected, you can control logging and notification properties for the following default packet-handling options:

- Spoofing attacks
- IP options
- Port probes
- Address space probes
- Incoming packets not handled
- Outgoing packets not handled

From Policy Manager:

1. Select **Setup** ⇒ **Intrusion Protection** ⇒ **Default Packet Handling**.
   The Default Packet Handling dialog box appears.
2. Click **Logging**.
3. Modify logging and notification properties according to your security policy preferences. Click **OK**.

Setting logging and notification for blocked sites and ports

You can control logging and notification properties for both blocked sites and blocked ports. The process is identical for both operations. The procedure below is for blocked sites.

From Policy Manager:

1. Select **Setup** ⇒ **Intrusion Protection** ⇒ **Blocked Sites**.
   The Blocked Sites dialog box appears.
2. Click **Logging**.
3. Modify logging and notification properties according to your security policy preferences. Click **OK**.

CHAPTER 13

Reviewing and Working with Log Files

Log files are a valuable tool for monitoring your network, identifying potential attacks, and taking action to address security threats and challenges. This chapter describes the procedures you use to work with log files, including viewing log files, searching for entries in them, and consolidating and copying logs.

The WatchGuard Security Event Processor (WSEP) controls logging, report schedules, and notification. It also provides timekeeping services for the Firebox. For more information about the WatchGuard Security Event Processor and configuring logging, see Chapter 12, "Setting Up Logging and Notification."

For more information on specific log messages, see the following collection of FAQs:
https://www.watchguard.com/support/advancedfaqs/log_main.asp

Log File Names and Locations

Log entries are stored on the primary and backup WatchGuard Security Event Processor (WSEP). By default, log files are placed in the WatchGuard installation directory in a subdirectory called `\logs`.

The log file to which the WSEP is currently writing records can be named in two ways. If the Firebox has a friendly name, the log files are named *FireboxName timestamp*.`wgl`. (You can give your Firebox a friendly name using the **Setup** ⇒**Name** option in Policy Manager.) If the Firebox does not have a friendly name, the log files are named *FireboxIP timestamp*.`wgl`.

In addition, the WSEP creates an index file using the same name as the log file, but with the extension `.idx1`. This file is located in the same directory as the log file. Both the `.wgl` and `.idx1` files are necessary if you want to use any monitoring or log display tool. For more information on the log file names, see the following FAQ:
https://www.watchguard.com/support/advancedfaqs/log_filename.asp

Viewing Files with LogViewer

The WatchGuard System Manager utility called LogViewer provides a display of log file data. You can view all log data page by page, or search and display by keyphrases or specific log fields.

Starting LogViewer and opening a log file

From Firebox System Manager:

1 Click the LogViewer icon (shown at right).
LogViewer opens and the Load File dialog box appears.



2 Browse to select a log file. Click **Open**.
By default, logs are stored in a subdirectory of the WatchGuard installation directory called \logs. LogViewer opens and displays the selected log file.

Setting LogViewer preferences

You can adjust the content and format of the display. From LogViewer:

1 Select **View** ⇒ **Preferences**.

2 Configure LogViewer display preferences as you choose.
For a description of each control on the General tab, right-click it and then click What's This?. You can also refer to the "Field Definitions" chapter in the *Reference Guide*. For information on the Filter Data tab, see "Displaying and Hiding Fields" on page 206.

Searching for specific entries

LogViewer has a search tool to enable you to find specific transactions quickly by keyphrase or field. From LogViewer:

By keyphrase

1. Select **Edit ⇒ Search ⇒ by Keyphrase**.
2. Enter an alphanumeric string. Click **Find**.
   LogViewer searches the entire log file and displays the results as either marked records in the main window or a separate filter window based on your selection.

By field

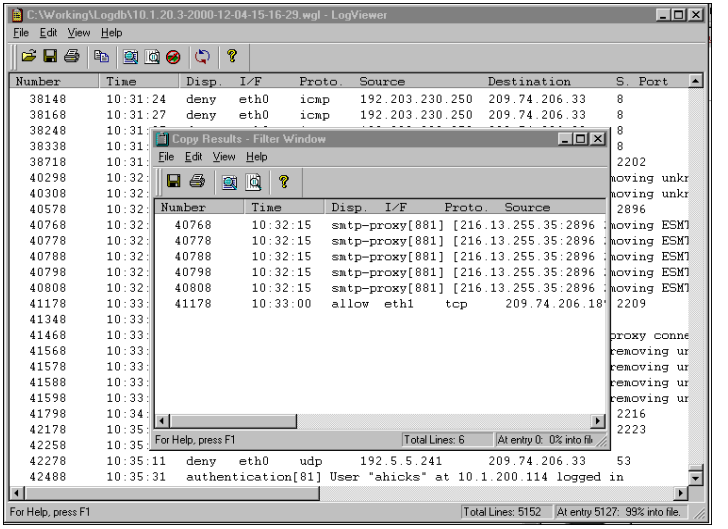
1. Select **Edit ⇒ Search ⇒ By Fields**.
2. Click directly under the **Field** column. Use the drop-down list that appears to select a field name.
3. Click the **Value** column. Either a text field or a drop-down list will appear, depending on the field you chose in step 2. Use the drop-down list to select a value, or type in a specific value.
4. Click **Search**.
   LogViewer searches the entire log file and displays the results as either marked records in the main window or a separate filter window based on your selection.

Copying and exporting LogViewer data

You can transfer log file data from LogViewer into another application. The data you choose to transfer is converted to a text file (`.txt`).

If you want to transfer specific log entries to another application, use the copy function. Use the export function if you want to transfer entire log files, or a filtered set of records (see next paragraph), to another application.

You can copy log entries to an interim window, called the LogViewer filter window, prior to exporting them. Within the filter window (shown on top of the LogViewer window in the figure on the next page) you can perform the same search functions as described in the previous section.


C:\Working\Logdb\10.1.20.3-2000-12-04-15-16-29.wgl - LogViewer
File Edit View Help
Number Time Disp. I/F Proto. Source Destination S. Port
38148 10:31:24 deny eth0 icmp 192.203.230.250 209.74.206.33 8
38168 10:31:27 deny eth0 icmp 192.203.230.250 209.74.206.33 8
Copy Results - Filter Window
File Edit View Help
Number Time Disp. I/F Proto. Source
40768 10:32:15 smtp-proxy[881] [216.13.255.35:2896
40778 10:32:15 smtp-proxy[881] [216.13.255.35:2896
40788 10:32:15 smtp-proxy[881] [216.13.255.35:2896
40798 10:32:15 smtp-proxy[881] [216.13.255.35:2896
40808 10:32:15 smtp-proxy[881] [216.13.255.35:2896
41178 10:33:00 allow eth1 tcp 209.74.206.18
For Help, press F1
Total Lines: 6
At entry 0: 0% into fil
42278 10:35:11 deny eth0 udp 192.5.5.241 209.74.206.33 53
42488 10:35:31 authentication[81] User "ahicks" at 10.1.200.114 logged in
For Help, press F1
Total Lines: 5152
At entry 5127: 99% into file.

Copying log data

1 Select the log entries you want to copy.

Use the SHIFT key to select a block of entries. Use the CTRL key to select multiple, non-adjacent entries.

2 To copy the entries for pasting into another application, select **Edit ⇒ Copy to clipboard**.

To copy the entries to the filter window prior to exporting them, select **Edit ⇒ Copy to Filter Window**.

Exporting log data

You can export log records from either the main window (all records) or the filter window.

1 Select **File ⇒ Export**.

The Save Main Window dialog box appears.

2 Select a location. Enter a file name. Click **Save**.

LogViewer saves the contents of the selected window to a text file.

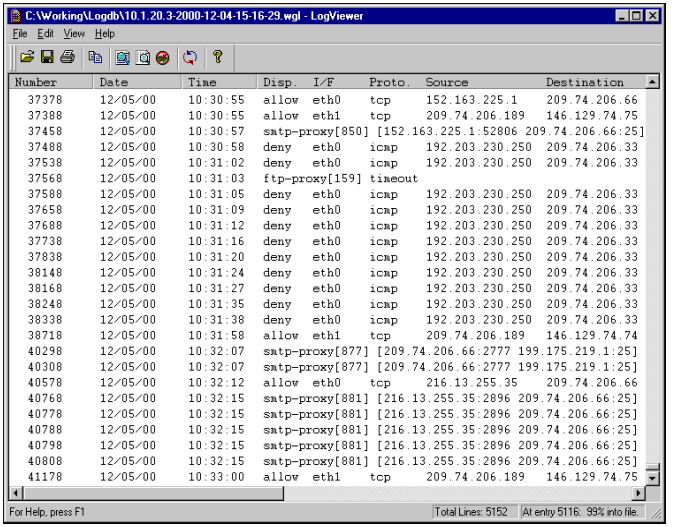
Displaying and Hiding Fields

The following figure shows an example of the type of display you normally see in LogViewer. Log entries sent to the WatchGuard log state the time stamp, host name, process name, and

the process ID before the log summary. Use the **Preferences** dialog box to show or hide columns displayed in LogViewer. From LogViewer:

1 Select **View** ⇒ **Preferences**. Click the **Filter Data** tab.

2 Select the checkboxes of the fields you would like to display. Clear the checkboxes of those columns you would like to hide.



The following describes each column and whether the default is for the field to appear (Show) or not appear (Hide):

Number

The sequence number in the file. Default = Hide

Date

The date the record entered the log file. Default = Show

Time

The time the record entered the log file. Default = Show
The Firebox receives the time from the log host. If the time noted in the log seems later or earlier than it should be, it is usually because the time zone is not set properly on either the log host or the Firebox. Because some installations contain Fireboxes in multiple time zones with a single log

host, the Firebox uses Greenwich Mean time received from the log host by way of the logging channel (controld). The local time for the log files is then computed on the log host based on the Firebox's time zone setting. To change the Firebox time zone, see "Setting the Time Zone" on page 48.

The rest of the columns vary according to the type of event displayed. The events of most frequency and interest, however, are packet events, which display data as shown below:

```
deny in eth0 339 udp 20 128 192.168.49.40
255.255.255.255 67 68 (bootpc)
```

The packet event fields are described here in order, from left to right.

Disposition

Default = Show. The disposition can be as follows:

- **Allow** — Packet was permitted by the current set of filter rules.
- **Deny** — Packet was dropped by the current set of filter rules.

Direction

Determines whether the packet was logged when it was received by the interface ("in") or when it was about to be transmitted by the Firebox ("out"). Default = Hide

Interface

The name of the network interface associated with the packet.
Default = Show

Total packet length

The total length of the packet in octets. Default = Hide

Protocol

Protocol name, or a number from 0 to 255. Default = Show

IP header length

Length, in octets, of the IP header for this packet. A header length that is not equal to 20 indicates that IP options were present. Default = Hide

TTL (time to live)

The value of the TTL field in the logged packet. Default = Hide

Source address
The source IP address of the logged packet. Default = Show

Destination address
The destination IP address of the logged packet. Default = Show

Source port
The source port of the logged packet, UDP or TCP only. Default = Show

Destination port
The destination port of the logged packet, UDP or TCP only. Default = Show

Details
Additional information appears after the previously described fields, including data about IP fragmentation, TCP flag bits, IP options, and source file and line number when in trace mode. If WatchGuard logging is in debug or verbose mode, additional information is reported. In addition, the type of connection may be displayed in parentheses. Default = Show

Working with Log Files

The Firebox continually writes messages to log files on the WatchGuard Security Event Processor (WSEP). Because current log files are always open, they cannot be copied, moved, or merged using traditional copy tools; you should use WSEP utilities to work with active log files.

Unlike other WatchGuard System Manager utilities, you cannot access the WatchGuard Security Event Processor user interface from Firebox System Manager. To open the WSEP Status/Configuration user interface:

- Right-click the WSEP icon (shown at right) in the Windows system tray and select **WSEP Status/ Configuration**. If the WSEP icon does not appear in the system tray, you can launch the WSEP from System Manager by selecting **Tools ⇒ Logging ⇒ Event Processor Interface**.



Consolidating logs from multiple locations

You can merge two or more log files into a single file. This merged file can then be used with Historical Reports, LogViewer, HostWatch, or some other utility to examine log data covering an extended period of time. From the WSEP Status/Configuration user interface:

1 Select **File ⇒ Copy or Merge log files**.

2 Click **Merge all files to one file**. Enter the name of the merged file.

3 Enter the files to merge in the **Files to Copy** box.
You can also use the Browse button to specify the files.

4 Enter the destination for the files in the **Copy to This Directory** box.

5 Click **Merge**.
The log files are merged and saved to the new file in the designated directory.

Copying log files

You can copy a single log file from one location to another, and you can copy the current, active log file. From the WSEP Status/Configuration user interface:

1 Select **File ⇒ Copy or Merge Log Files**.

2 Click **Copy each file individually**.

3 Enter the file to copy in the **Files to Copy** box.

4 Enter the destination for the file in the **Copy to This Directory** box.

5 Click **Copy**.
The log file is copied to the new directory with the same file name.

Forcing the rollover of log files

Log rollover refers to new log files being created while old ones are deleted or archived. In general, log files roll over based on WSEP Status/Configuration settings. For more information, see “Setting the interval for log rollover” on page 195. However, you may occasionally want to force the rollover of a log file.

- From the WSEP Status/Configuration user interface, select **File ⇒ Roll Current Log File**.
  The old log file is saved as Firebox IP Time Stamp.wgl or Firebox Name Time Stamp.wgl. The Event Processor continues writing new records to Firebox IP.wgl or Firebox Name.wgl.

Saving log files to a new location

Although log files are, by default, stored in a subdirectory of the WatchGuard installation directory called `/logs`, you can change this destination by using a text editor to edit the `controld.wgc` file.

1. Open a text editor, such as Microsoft Wordpad.
2. Use the text editor to open the `controld.wgc` file in the WatchGuard installation directory.
   The default location is C:\Program Files\WatchGuard\controld.wgc.
3. Look for a line reading `logdir: logs`. Change `logs` to the complete or relative path name of the new destination.
   For example, to change the destination to an archive directory with the subdirectory WGLogs on the D: drive, the syntax is logdir: D:\Archive\WGLogs.
4. Save your changes and exit the text editor.
5. Stop and restart the WatchGuard Security Event Processor: Right-click the WatchGuard Security Event Processor in the Windows desktop tray. Select **Stop Service**. Right-click the icon again and select **Start Service**.
   New log files will be created in the specified directory. You can also move any existing log files from the old location to the new one to avoid confusion.

Setting log encryption keys

The log connection (but not the log file) between the Firebox and an event processor is encrypted for security purposes. Both the management station and the WatchGuard Security Event Processor must have the same encryption key. From the WSEP Status/Configuration user interface:

1. Select **File ⇒ Set Log Encryption Key**.
   The Set Log Encryption Key dialog box appears.
2. Enter the log encryption key in the first box. Enter the same key in the box beneath it to confirm.

Sending logs to a log host at another location

Because they are encrypted by the Firebox, you can send log files over the Internet to a log host at another office. You can even send this traffic over the Internet from the Firebox at one office to the log host behind a second Firebox at a remote office. One application of this feature might involve configuring the Firebox at a remote office to store its logs on a log host behind the Firebox at the main office. To do this, you must configure the Firebox at the remote office such that it knows where and how to send the log files. The main office Firebox must be configured to allow the log messages through the firewall to the log host.

On the main office Firebox:

1 Open Policy Manager with the current configuration file.

2 On the toolbar, click the Add Service icon (shown at right).



You can also select Edit ⇒ Add Service. The Services dialog box appears.

3 Expand **Packet Filters**.

4 Select **WatchGuard-Logging**. Click **Add**. Click **OK**.

5 On the Incoming tab, select **Enabled and Allowed**.

6 Under the **To** list, click **Add**.

7 Click **NAT**. Enter the external IP address of the main office Firebox in the **External IP Address** box. Enter the IP address of the log host behind the main office Firebox in the **Internal IP Address** box.

8 Click **OK** to close the **Add Static NAT** dialog box. Click **OK** to close the **Add Address** dialog box. Click **OK** to close the **WatchGuard-Logging Properties** dialog box.

9 Save the new configuration to the main office Firebox.

On the remote office Firebox:

1 Open Policy Manager with the current configuration file.

2 Select **Setup ⇒ Logging**. Click **Add**.

3 Enter the external IP address of the main office Firebox and log encryption key of the log host on the network protected by the main office Firebox.

4 Click **OK** to close the **Add IP Address** dialog box. Click **OK** again to close the **Logging Setup** dialog box.

5 Save the new configuration to the remote office Firebox.

On the log host:

You must use the same log encryption key on the remote office Firebox as is configured on the log host protected by the main office Firebox. To modify the log encryption key on the log host, see “Setting log encryption keys” on page 211.

You should see the IP address for the remote office Firebox in the list as soon as it connects. However, it will not appear until the remote office Firebox has been properly configured.

CHAPTER 14

Generating Reports of Network Activity

Accounting for Internet usage can be a challenging network administration task. One of the best ways to provide hard data for accounting and management purposes is to generate detailed reports showing how the Internet connection is being used and by whom.

A good report generation facility should be able to identify and summarize key issues such as:

- When do I need a wider bandwidth connection to the Internet and why?
- What usage patterns are users developing and how do those patterns relate to the security of the network and the goals of the corporation?
- How do current user patterns reflect the values and concerns of the corporation in regard to creating a productive workplace?

Historical Reports is a reporting tool that creates summaries and reports of Firebox log activity. It generates these reports using the log files created by and stored on the WatchGuard Security Event Processor (WSEP).

You can customize reports to include exactly the information you need in a form that is most useful to you. Using the advanced features of Historical Reports, you can define a pre-

cise time period for a report, consolidate report sections to show activity across a group of Fireboxes, and set properties to display the report data according to your preferences.

Creating and Editing Reports

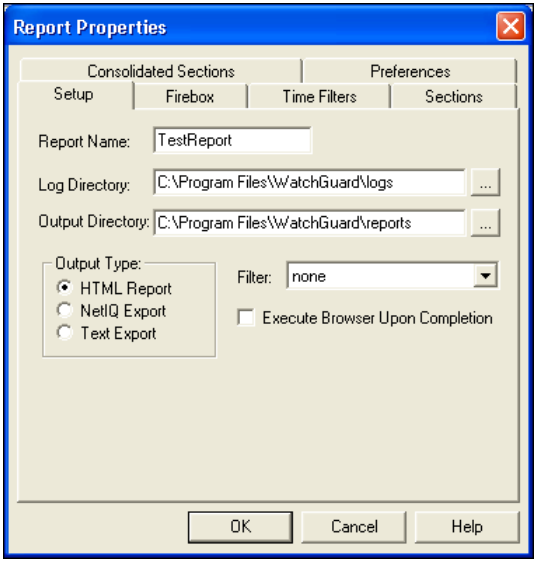
To start Historical Reports, from Firebox System Manager, click the Historical Reports icon (shown at right). You can also start Historical Reports from the installation directory. The file name is `WGReports.exe`.



Starting a new report

From Historical Reports:

1 Click **Add**.
The Report Properties dialog box appears.



2 Enter the report name.
The report name will appear in Historical Reports, the WatchGuard Security Event Processor, and the title of the output.

3 Use the **Log Directory** text box to define the location of log files.
The default location for log files is the \logs subdirectory of the WatchGuard installation directory.

4 Use the **Output Directory** text box to define the location of the output files.
The default location for output files is the \reports subdirectory of the WatchGuard installation directory.

5 Select the output type: HTML Report, NetIQ Export, or Text Export.
For more information on output types, see "Exporting Reports" on page 220.

6 Select the filter.
For more information on filters, see "Using Report Filters" on page 222.

7 If you selected the HTML output type and you want to see the main page of the report upon completion, select the checkbox marked **Execute Browser Upon Completion**.

8 Click the **Firebox** tab.

9 Enter the Firebox IP address or a unique name. Click **Add**.
When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

10 Specify report preferences as explained in the remaining sections in this chapter.

11 When you are done defining report properties, click **OK**.
The name of the report appears in the Reports list.

Editing an existing report

At any time, you can modify the properties of an existing report. From Historical Reports:

1 Select the report to modify. Click **Edit**.
The Report Properties dialog box appears.

2 Modify report properties according to your preferences.
For a description of each property, right-click it, and then click What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

Deleting a report

To remove a report from the list of available reports, highlight the report. Click **Remove**. This command removes the `.rep` file from the `reports` directory.

Viewing the reports list

To view all reports generated, click **Reports Page**. This launches your default browser with the HTML file containing the main report list. You can navigate through all the reports in the list.

Specifying a Report Time Span

When running Historical Reports, the default is to run the report across the entire log file. You can use the drop-down list on the **Time Filters** dialog box to select from a group of pre-set time periods, such as "yesterday" and "today." You can also manually configure the start and end times so the report covers only the specific time frame you want to examine.

1 From the **Report Properties** dialog box, click the **Time Filters** tab.

2 Select the time stamp option that will appear on your report: **Local Time** or **GMT**.

3 From the **Time Span** drop-down list, select the time you want the report to cover.
If you chose anything but Specify Time Filters, click OK.
If you chose Specify Time Filters, click the Start and End drop-down lists and select a start time and end time, respectively.

4 Click **OK**.

Specifying Report Sections

Use the **Sections** tab on the **Report Properties** dialog box to specify the type of information you want to be included in reports. From Historical Reports:

1 Click the **Sections** tab.

2 Select the checkboxes for sections to be included in the report.
For a description of each section, see "Report Sections and Consolidated Sections" on page 224.

3 To run authentication resolution on IP addresses, select the checkbox marked **Authentication Resolution on IP addresses**.
If user authentication is not enabled, you will not have the information in your logs to perform authentication resolution on IP

addresses. However, generating a report when resolution is enabled will take considerably more time.

4 To run DNS resolution on IP addresses, select the checkbox marked **DNS Resolution on IP addresses**.

Consolidating Report Sections

The **Sections** tab defines the types of information to be included in a report on each of a group of Fireboxes: a vertical look at the data. You can also specify parameters that consolidate information for a group of Fireboxes: a horizontal (cumulative) view of data. To consolidate report sections:

1 From the **Report Properties** dialog box, select the **Consolidated Sections** tab.
The tab contains a list of report sections that can be consolidated. Brief definitions of the contents of these sections are available in "Report Sections and Consolidated Sections" at the end of this chapter.

2 Click the boxes next to the items you want to include in the consolidated report or click a checked box to clear it.

3 Click **OK**.

Setting Report Properties

Reports contain either Summary sections or Detail sections. Each can be presented in different ways to better focus on the specific information you want to view. Detail sections are reported only as text files with a user-designated number of records per page. Summary sections can also be presented as graphs whose elements are user-defined. To set report properties:

1 From the **Report Properties** dialog box, select the **Preferences** tab.

2 Enter the number of elements to graph in the report.
The default is 10.

3 Enter the number of elements to rank in the table.
The default is 100.

4 Select the style of graph to use in the report.

5 Select the manner in which you want the proxied summary reports sorted: bandwidth or connections.

6 Enter the number of records to display per page for the detailed sections.

The default is 1,000 records. A larger number than this might crash the browser or cause the file to take a long time to load.

7 Click **OK**.

Setting a Firebox friendly name for reports

You can give the Firebox a friendly name to be used in reports. If you do not specify a name, the Firebox's IP address is used. From Policy Manager:

1 Select **Setup** ⇒ **Name**.

The Firebox Name dialog box appears.

2 Enter the friendly name of the Firebox. Click **OK**.

Exporting Reports

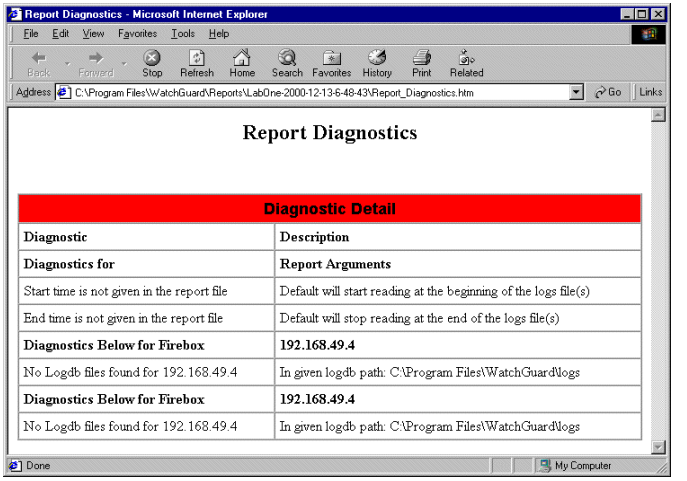
Reports can be exported to three formats: HTML, NetIQ, and text.

All reports are stored in the path *drive*:*WatchGuard Install Directory*\`Reports`. Under the Reports directory are subdirectories that include the name and time of the report. Each report is filed in one of these subdirectories.

Exporting reports to HTML format

When you select **HTML Report** from the **Setup** tab on the **Report Properties** dialog box, the report output is created as HTML files. A JavaScript menu is used to easily navigate the different report sections. (JavaScript must be enabled on the browser so you can review the report menu.)

The following figure shows how the report might appear in the browser.


Report Diagnostics - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Print Related
Address C:\Program Files\WatchGuard\Reports\LabOne-2000-12-13-6-48-43\Report_Diagnostics.htm
Go Links
Report Diagnostics
Diagnostic Detail
Diagnostic
Description
Diagnostics for
Report Arguments
Start time is not given in the report file
Default will start reading at the beginning of the logs file(s)
End time is not given in the report file
Default will stop reading at the end of the logs file(s)
Diagnostics Below for Firebox
192.168.49.4
No Logdb files found for 192.168.49.4
In given logdb path: C:\Program Files\WatchGuard\logs
Diagnostics Below for Firebox
192.168.49.4
No Logdb files found for 192.168.49.4
In given logdb path: C:\Program Files\WatchGuard\logs
Done
My Computer

Exporting reports to NetIQ format

NetIQ calculates information differently than WatchGuard Historical Reports. While Historical Reports counts the number of transactions that occur on Port 80, NetIQ calculates the number of URL requests. These numbers vary because multiple URL requests may go over the same Port 80 connection.

NOTE

WatchGuard HTTP proxy logging must be turned on to supply NetIQ the logging information required for its reports.

The report appears in the following path:

drive: *WatchGuard Install Directory*\`Reports`

Exporting a report to a text file

When you select **Text Export** from the **Setup** tab on the **Report Properties** dialog box, the report output is created as a comma-delimited format file, which you can then use in other programs such as databases and spreadsheets. The report appears as a `.txt` file in the following path:

drive:*WatchGuard Install Directory*\`Reports`*Report Directory*

Using Report Filters

By default, a report displays information on the entire content of a log file. At times, however, you may want to view information only about specific hosts, services, or users. Use report filters to narrow the range of data reported.

Filters can be one of two types:

Include
Creates a report that includes only those records that meet the criteria set in the **Host**, **Service**, or **User Report Filters** tabs.

Exclude
Creates a report that excludes all records that meet the criteria set in the **Host**, **Service**, or **User Report Filter** tabs.

You can filter an Include or Exclude report based on three criteria:

Host
Filter a report based on host IP address.

Port
Filter a report based on service name or port number.

User
Filter a report based on authenticated username.

Creating a new report filter

Use Historical Reports to create a new report filter. Filters are stored in the WatchGuard installation directory, in the subdirectory `report-defs` with the file extension `.ftr`.

From Historical Reports:

1 Click **Filters**. Click **Add**.

2 Enter the name of the filter as it will appear in the **Filter** drop-down list in the **Report Properties Setup** tab. This name should easily identify the filter.

3 Select the filter type.
An Include filter displays only those records meeting the criteria set on the Host, Service and User tabs. An Exclude filter displays all records except those meeting the criteria set on the Host, Service, and User tabs.

4 Complete the **Filter** tabs according to your report preferences.

For a description of each control, right-click it, and then click What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

5 When you are finished modifying filter properties, click **OK**.

The name of the filter appears in the Filters list. The Filter Name.ftr file is created in the report-defs directory.

Editing a report filter

At any time, you can modify the properties of an existing filter. From the **Filters** dialog box in Historical Reports:

1 Highlight the filter to modify. Click **Edit**.

The Report Filter dialog box appears.

2 Modify filter properties according to your preferences.

For a description of each property, right-click it, and then click What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

Deleting a report filter

To remove a filter from the list of available filters, highlight the filter. Click **Delete**. This command removes the `.ftr` file from the `\report-defs` directory.

Applying a report filter

Each report can use only one filter. To apply a filter, open the report properties. From Historical Reports:

1 Select the report for which you would like to apply a filter. Click **Edit**.

2 Use the **Filter** drop-down list to select a filter.

Only filters created using the Filters dialog box appear in the Filter drop-down list. For more information, see "Creating a new report filter" on page 222.

3 Click **OK**.

The new report properties are saved to the ReportName.rep file in the report-defs directory. The filter will be applied the next time the report is run.

Scheduling and Running Reports

WatchGuard offers two methods to run reports: manually at any time or scheduled automatically using the WatchGuard Security Event Processor (WSEP).

Scheduling a report

You can schedule the WSEP to automatically generate reports about network activity. To schedule reports:

1. Right-click the WSEP desktop tray icon. Select **WSEP Status/Configuration**.
2. Click the **Reports** tab.
3. Select a report to schedule.
4. Select a time interval.
   For a custom interval, select Custom and then enter the interval in hours.
5. Select the first date and time the report should run.
   The report will run automatically at the time selected and then at each selected interval thereafter.
6. Click **OK**.

Manually running a report

At any time, you can run one or more reports using Historical Reports. From Historical Reports:

1. Select the checkbox next to each report you would like to generate.
2. Click **Run**.

Report Sections and Consolidated Sections

You can use Historical Reports to build a report that includes one or more sections. Each section represents a discrete type of information or network activity.

You can consolidate certain sections to summarize particular types of information. Consolidated sections summarize the activity of all devices being monitored as a group as opposed to individual devices.

Report sections

Report sections can be divided into two basic types:

- **Summary** – Sections that rank information by bandwidth or connections.
- **Detailed** – Sections that display all activity with no summary graphs or ranking.

The following is a listing of the different types of report sections and consolidated sections.

Firebox Statistics
A summary of statistics on one or more log files for a single Firebox.

Authentication Detail
A detailed list of authenticated users sorted by connection time. Fields include: authenticated user, host, start date of authenticated session, start time of authenticated session, end time of authenticated session, and duration of session.

Time Summary — Packet Filtered
A table, and optionally a graph, of all accepted connections distributed along user-defined intervals and sorted by time. If you choose the entire log file or specific time parameters, the default time interval is daily. Otherwise, the time interval is based on your selection.

Host Summary — Packet Filtered
A table, and optionally a graph, of internal and external hosts passing packet-filtered traffic through the Firebox sorted either by bytes transferred or number of connections.

Service Summary
A table, and optionally a graph, of traffic for each service sorted by connection count.

Session Summary — Packet Filtered
A table, and optionally a graph, of the top incoming and outgoing sessions, sorted either by byte count or number of connections. The format of the session is: client -> server : service. If the connection is proxied, the service is represented in all capital letters. If the connection is packet filtered, Historical Reports attempts to resolve the server port

to a table to represent the service name. If resolution fails, Historical Reports displays the port number.

Time Summary — Proxied Traffic
A table, and optionally a graph, of all accepted connections distributed along user-defined intervals and sorted by time. If you choose the entire log file or specific time parameters, the default time interval is daily. Otherwise, the time interval is based on your selection.

Host Summary — Proxied Traffic
A table, and optionally a graph, of internal and external hosts passing proxied traffic through the Firebox, sorted either by bytes transferred or number of connections.

Proxy Summary
Proxies ranked by bandwidth or connections.

Session Summary — Proxied Traffic
A table, and optionally a graph, of the top incoming and outgoing sessions, sorted either by byte count or number of connections. The format of the session is: client -> server : service. If the connection is proxied, the service is represented in all capital letters. If the connection is packet filtered, Historical Reports attempts to resolve the server port to a table to represent the service name. If resolution fails, Historical Reports displays the port number.

HTTP Summary
Tables, and optionally a graph, of the most popular external domains and hosts accessed using the HTTP proxy, sorted by byte count or number of connections.

HTTP Detail
Tables for incoming and outgoing HTTP traffic, sorted by time stamp. The fields are Date, Time, Client, URL Request, and Bytes Transferred.

SMTP Summary
A table, and optionally a graph, of the most popular incoming and outgoing email addresses, sorted by byte count or number of connections.

SMTP Detail
A table of incoming and outgoing SMTP proxy traffic, sorted by time stamp. The fields are: Date, Time, Sender, Recipient(s), and Bytes Transferred.

FTP Detail
Tables for incoming and outgoing FTP traffic, sorted by time stamp. The fields are Date, Time, Client, Server, FTP Request, and Bandwidth.

Denied Outgoing Packet Detail
A list of denied outgoing packets, sorted by time. The fields are Date, Time, Type, Client, Client Port, Server, Server Port, Protocol, and Duration.

Denied Incoming Packet Detail
A list of denied incoming packets, sorted by time. The fields are Date, Time, Type, Client, Client Port, Server, Server Port, Protocol, and Duration.

Denied Packet Summary
Multiple tables, each representing data on a particular host originating denied packets. Each table includes time of first and last attempt, type, server, port, protocol, and number of attempts. If only one attempt is reported, the last field is blank.

Denied Service Detail
A list of times a service was attempted to be used but was denied. The list does not differentiate between Incoming and Outgoing.

WebBlocker Detail
A list of URLs denied due to WebBlocker implementation, sorted by time. The fields are Date, Time, User, Web Site, Type, and Category.

Denied Authentication Detail
A detailed list of failures to authenticate, sorted by time. The fields are Date, Time, Host, and User.

IPS Blocked Sites
A list of IPS blocked sites.

Consolidated sections

Network Statistics
A summary of statistics on one or more log files for all devices being monitored.

Time Summary — Packet Filtered
A table, and optionally a graph, of all accepted connections distributed along user-defined intervals and sorted by time. If you choose the entire log file or specific time parameters, the default time interval is daily. Otherwise, the time interval is based on your selection.

Host Summary — Packet Filtered
A table, and optionally a graph, of internal and external hosts passing packet-filtered traffic, sorted either by bytes transferred or number of connections.

Service Summary
A table, and optionally a graph, of traffic for all services sorted by connection count.

Session Summary — Packet Filtered
A table, and optionally a graph, of the top incoming and outgoing sessions, sorted either by byte count or number of connections. The format of the session is: client -> server : service. If the connection is proxied, the service is represented in all capital letters. If the connection is packet filtered, Historical Reports attempts to resolve the server port to a table to represent the service name. If resolution fails, Historical Reports displays the port number.

Time Summary — Proxied Traffic
A table, and optionally a graph, of all accepted proxied connections distributed along user-defined intervals and sorted by time. If you choose the entire log file or specific time parameters, the default time interval is daily. Otherwise, the time interval is based on your selection.

Host Summary — Proxied Traffic
A table, and optionally a graph, of internal and external hosts passing proxied traffic, sorted either by bytes transferred or number of connections.

Proxy Summary

Proxies ranked by bandwidth or connections.

Session Summary — Proxied Traffic

A table, and optionally a graph, of the top incoming and outgoing sessions sorted either by byte count or number of connections. The format of the session is: client -> server : service. If proxied, connections show the service in all capital letters. If resolution fails, Historical Reports displays the port number.

HTTP Summary

Tables, and optionally graphs, of the most frequented external domains and hosts accessed using the HTTP proxy, sorted by byte count or number of connections.

CHAPTER 15

Controlling Web Site Access

WebBlocker is a feature of WatchGuard System Manager that works in conjunction with the HTTP proxy to provide Web site filtering capabilities. It enables you to exert fine control over the Web surfing in your organization. You can designate which hours in the day users are free to access the Web and which categories of Web sites they are restricted from visiting. For more information on WebBlocker, see the following collection of FAQs:
https://www.watchguard.com/support/advancedfaqs/web_main.asp

MUVPN and RUVPN with PPTP users can now be routed through the outgoing HTTP proxy.

Getting Started with WebBlocker

You must complete several tasks before you can configure the Firebox to use WebBlocker.

Installing the WebBlocker server

You install the WebBlocker server when you first run the setup program for WatchGuard System Manager, as described in "Setting Up the Management Station" on page 31. By default, the setup program installs the WebBlocker server on the same

server as the WatchGuard Security Event Processor. However, to preserve performance if you are running WatchGuard System Manager under high load conditions, consider installing the WebBlocker server on a dedicated server running Windows NT 4.0, Windows 2000, or Windows XP.

To install the WebBlocker server on a dedicated platform, rerun the setup program on the dedicated server and—on the Select Components screen—unselect all components except the WebBlocker server.

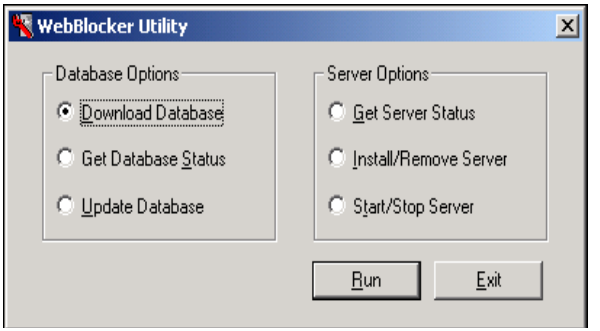
You must start the WebBlocker server for WebBlocker requests from the Firebox to be processed.

Downloading the database using WebBlocker Utility

After you install the WebBlocker server, you are asked whether you want to run the WebBlocker utility. Click **Yes**. The **WebBlocker Utility** dialog box appears, as shown in the following figure. Select **Download Database** to download the current database.

NOTE

The WebBlocker database is over 60 MB in size and may take 30 minutes or more to download.



You can run the WebBlocker utility at any time to:

- Download a new version of the database.
- View the current database status
- Upload the database

- View the current WebBlocker server status
- Install or remove the server
- Start or stop the server

To run the WebBlocker utility, select **Start** ⇒ **Programs** ⇒ **WatchGuard** ⇒ **WebBlocker Utility**.

Configuring the WatchGuard service icon

Because WebBlocker relies on copying updated versions of the WebBlocker database to the event processor, you must configure the WatchGuard service setting **Allow Outgoing to Any**. It is possible to narrow this setting and use the IP address of webblocker.watchguard.com. However, this address may change without notice.

Add an HTTP service

To use WebBlocker, add the Proxied-HTTP, Proxy, or HTTP service. WatchGuard recommends using Proxied-HTTP, which provides filtering on all ports. (HTTP without the Proxy service manages only port 80.) WebBlocker takes precedence over other settings in the HTTP or Proxy services. If the HTTP service allows outgoing from Any to Any but WebBlocker settings are set to "Block All URLs," all Web access is blocked. For information on adding an HTTP proxy service, see "Adding a proxy service for HTTP" on page 141.

Configuring the WebBlocker Service

WebBlocker is a built-in feature of several services, including HTTP, Proxied HTTP, and Proxy. When WebBlocker is installed, five tabs appear in the service's **Properties** dialog box:

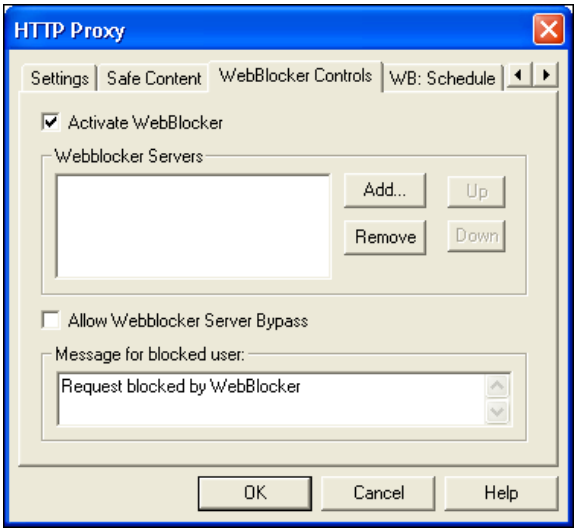
- WebBlocker Controls
- WB: Schedule
- WB: Operational Privileges
- WB: Non-operational Privileges
- WB: Exceptions

Activating WebBlocker

To start using WebBlocker, you must activate the feature. From Policy Manager:

1 Double-click the service icon you are using for HTTP. Click the **Properties** tab. Click **Settings**.
The service's dialog box appears.

2 Click the **WebBlocker Controls** tab.
The tab appears, as shown in the following figure.



3 Select the checkbox marked **Activate WebBlocker**.

4 Next to the **WebBlocker Servers** box, click **Add**.

5 In the dialog box that appears, type the IP address of the server in the **Value** field. Click **OK**.
If you want to add additional WebBlocker servers, see "Installing Multiple WebBlocker Servers" on page 238.

Allowing WebBlocker server bypass

By default, if the WebBlocker server does not respond, HTTP traffic (Outbound) is denied. To change this such that all outbound HTTP traffic is allowed if a WebBlocker server is not recognized, on the **WebBlocker Controls** tab, select **Allow WebBlocker Server Bypass**.

The **Allow WebBlocker Server Bypass** option is global. If you set it in one HTTP service, it applies to all other HTTP proxy services you might have.

Configuring the WebBlocker message

Use the field marked **Message for blocked user** to define the text string displayed in end users' browsers when they attempt to open a blocked Web site. The text string must be plain text and cannot contain HTML or the greater than (>) or less than (<) characters. The following metacharacters are permitted:

%u
The full URL of the denied request.

%s
Block status, or the reason the request was blocked. The possible statuses are: **host**, **host/directory**, **all web access blocked**, **denied**, **database not loaded**.

%r
The WebBlocker category or categories causing the denial.

For example, the following entry in the field will display the URL, the status, and the category:

```
Request for URL %u denied by WebBlocker: %s
blocked for %r.
```

With this entry in the **Message for blocked user** field, the following string might appear in a user's browser:

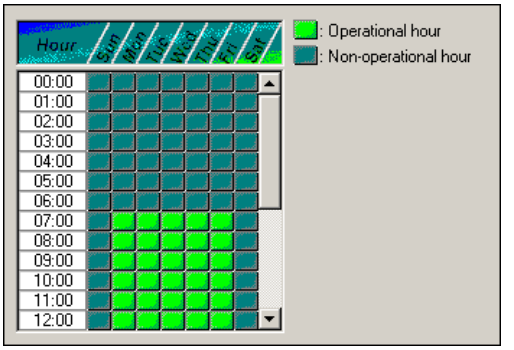
```
Request for URL www.badsite.com denied by
WebBlocker: host blocked for violence/
profanity.
```

Scheduling operational and non-operational hours

WebBlocker provides two separately configurable time blocks—operational hours and non-operational hours. Typically, operational hours are an organization's normal hours of operation and non-operational hours are when an organization is not conducting its normal business. Use these time blocks to build rules about when different types of sites are to be blocked. For example, you might block sports sites during business hours, but allow access at lunch time, evenings, and weekends.

From the proxy's dialog box:

1 Click the **WB: Schedule** tab.
The tab appears, as shown in the following figure.



2 Click hour blocks to toggle from **Operational** to **Non-operational**.

NOTE

The operational and non-operational hours schedule is dependent on the time zone settings. WebBlocker defaults to GMT unless you have set a Firebox time zone. For information on setting the Firebox time zone, see "Setting the Time Zone" on page 48.

Setting privileges

WebBlocker differentiates URLs based on their content. Select the types of content accessible during operational and non-operational hours using the **Privileges** tabs. The options are identical for Operational and Non-operational. From the proxy's dialog box:

1 Click the **WB: Operational Privileges** tab or the **WB: Non-operational Privileges** tab.

2 Select the content type checkboxes for the categories you would like to block.

Creating WebBlocker exceptions

WebBlocker provides an exceptions control to override any of the WebBlocker settings. Exceptions take precedence over all other WebBlocker rules; you can add sites that you want to be

allowed or denied above and beyond other WebBlocker settings. Sites listed as exceptions apply only to HTTP traffic and are not related to the Blocked Sites list.

The exceptions option maintains a list of IP addresses that you want to either specifically allow or deny, regardless of other WebBlocker settings. You can specify exceptions by domain name, network address, or host IP address. You can also fine-tune your exceptions by specifying a port number, path name, or string which is to be blocked for a particular Web site. For example, if you wanted to block only www.sharedspace.com/~dave, because Dave's site contains nude pictures, you would enter "`~dave`" to block that directory of sharedspace.com. This would still allow users to have access to www.sharedspace.com/~julia, which contains a helpful article on increasing productivity.

If you wanted to block any sexually explicit content that might be on sharedspace.com, you might enter `*sex`, to block a Web page such as www.sharedspace.com/~george/sexy.htm. By placing an asterisk (*) in front of the string you want to match, it will be matched if that string appears anywhere in the location part of the URL. However, you cannot enter `*sex` in the pattern section, and expect to block all URLs that contain the word "sex." The * option can be used only to modify the exceptions within a specific URL. For example, you can block www.sharedspace.com/*sex and expect that www.sharedspace/sexsite.html will be blocked.

NOTE

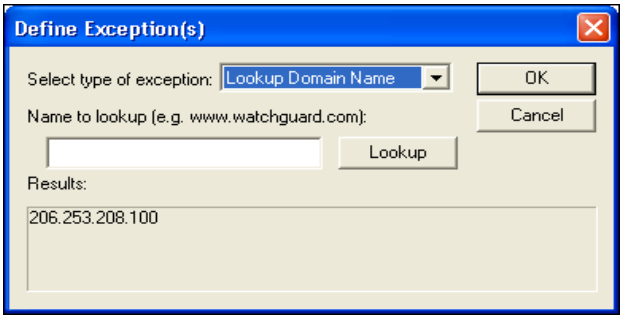
This WebBlocker feature is applicable only for outbound requests to access web sites. You cannot use WebBlocker exceptions to make an internal host exempt from WebBlocker rules.

From the **HTTP Proxy** dialog box:

1 Click the **WB: Exceptions** tab (you might need to use the arrow keys at the right of the dialog box to see this tab).

2 In the **Allowed Exceptions** section, click **Add**.
The Define Exceptions dialog box appears.

3 Select the type of exception: host address, network address, or enter URL. You can also use the **Lookup Domain Name** option to determine the IP address of a domain.



4 To allow a specific port or directory pattern, enter the port or string to be allowed.

When typing IP addresses, type the digits and periods in sequence. Do not use the TAB or arrow key to jump past the periods. For more information on entering IP addresses, see "Entering IP addresses" on page 37.

5 In the **Denied Exceptions** section, click **Add**. Specify the host address, network address, or URL to be denied.

To block a specific string to be denied for a domain, select Host Address. To block a specific directory pattern, enter the string to be blocked (for example, "*poker").

6 To remove an item from either the Allow or the Deny list, select the address. Click the corresponding **Remove** button.

Managing the WebBlocker Server

The WebBlocker server is installed as a Windows Service and can be started or stopped from the Services application located in the Windows Control Panel Program Group.

Installing Multiple WebBlocker Servers

You can install two or more WebBlocker servers in a failover configuration. If the primary WebBlocker server fails, the Firebox

automatically fails over to the first server in the **WebBlocker Servers** box, as shown in "Activating WebBlocker" on page 234.

To add additional WebBlocker servers:

1 On the **WebBlocker Controls** tab in the **HTTP Proxy** dialog box, click **Add**.

2 In the dialog box that appears, type the IP address of the server in the **Value** field. Click **OK**.

You can use the Up and Down buttons to change the position of the servers in the list.

When operating two or more WebBlocker servers in a failover mode, the time between failovers may take up to two minutes.

Automating WebBlocker Database Downloads

The most effective way to routinely download and update your WebBlocker database is to use Windows Task Scheduler. To do this, add a process called WebDBdownload.bat, which appears in your WatchGuard directory under the WBServer folder:

1 Open Control Panel and select **Scheduled Tasks**. (If it is not listed, see "Installing Scheduled Tasks," in the following section.)

2 Select **Add Scheduled Task**.

3 The Scheduled Tasks wizard launches. Click **Next**.

4 On the next screen, which shows a list of programs to select from, select **Browse**.

5 Navigate to your WatchGuard directory and then into WBServer. Select `WebDBdownload.bat`.

6 Specify how often you want to perform this task. WatchGuard suggests you update your database every day, although you can do it less often if you have bandwidth concerns. Click **Next**.

7 Enter a start time for the process. Because these downloads are close to 60 megabytes, choose a time outside normal work hours.

8 Select the frequency you want for this task. WatchGuard recommends you perform updates on weekdays, because the database is not updated on weekends.

9 Select a suitable start date. Click **Next**.

10 Enter the user name and passwords that this process requires to run. Make sure this user has access to the proper files. Click **Next**.

11 Review your entries. Click **Finish**.

Installing Scheduled Tasks

If you are running Windows NT 4.0, you might need to manually install Scheduled Tasks:

1 Open Control Panel and select **Add/Remove Programs**.

2 From the list, select **Microsoft Internet Explorer**.

3 When prompted, select **Add a component**.

4 A list of software appears (this may take a few minutes). If you're using Internet Explorer 4.0, under Additional Explorer Enhancements, select **Task Scheduler**. If you're using Internet Explorer 5.0 or later, select **Offline Browsing Pack**.

If the message "cannot find Windows Update Files on this computer" appears, open Internet Explorer, go to the **Tools** menu, and select **Windows Update**. This takes you to the Microsoft Web site, where you can download and install the appropriate software.

After installation, Scheduled Tasks appears under My Computer.

CHAPTER 16

Connecting with Out-of-Band Management

WatchGuard System Manager out-of-band (OOB) management feature enables the management station to communicate with a Firebox by way of a modem (not provided with the Firebox) and telephone line. OOB is useful for remotely configuring a Firebox when access through the Ethernet interfaces is unavailable.

Connecting a Firebox with OOB Management

To connect to the Firebox using OOB management, you must:

- Connect the management station to a modem — Connect a modem between the serial port on the management station and an analog telephone line.
- Connect the Firebox modem — Connect an external or PCMCIA (also known as PC card) modem to the Firebox. External modems must be attached to the Console port of the Firebox.
- Enable the management station for dial-up networking connections.
- Set Firebox network configuration properties.

Enabling the Management Station

For a dial-up PPP connection to work between a management station and a Firebox, you must configure the management station to use a PPP connection. There are separate procedures for configuring a PPP connection on the Windows NT, Windows 2000, and Windows XP platforms.

Preparing a Windows NT management station for OOB

Install the Microsoft Remote Access Server (RAS) on the management station.

1. Attach a modem to your computer according to the manufacturer's instructions.
2. From the Windows NT Desktop, select **Start** ⇒ **Settings** ⇒ **Control Panel**.
3. Double-click **Network**.
4. Click **Add**.
   The Select Network Service dialog box appears.
5. Click **Remote Access Server**. Click **OK**.
   Follow the rest of the prompts to complete the installation. If Dial-Up Networking is not already installed, you will be prompted to install it.

Preparing a Windows 2000 management station for OOB

Before configuring the management station, you must first install the modem. If the modem is already installed, go to the instructions for configuring the dial-up connection.

Install the modem

1. From the Desktop, click **Start** ⇒ **Settings** ⇒ **Control Panel** ⇒ **Phone and Modem Options**.
2. Click the **Modems** tab.
3. Click **Add**.
   The Add/Remove Hardware Wizard appears.
4. Follow the wizard through, completing the information requested.
   You will need to know the name and model of the Firebox modem and the modem speed.

5 Click **Finish** to complete the modem installation.

Configure the dial-up connection

1 From the Desktop, click **My Network Places** ⇒ **Network and Dial-up Connections** ⇒ **Make New Connection**.
The Network Connection wizard appears.

2 Click **Next**. Select **Dial up to Private Network**. Click **Next**.

3 Enter the telephone number of the line connected to the modem in the Firebox. Click **Next**.

4 Choose the proper designation for your connection. Click **Next**.

5 Enter a name for your connection.
This can be anything that reminds you of the icon's purpose—OOB Connection, for example.

6 Click **Finish**.

7 Click either **Dial** or **Cancel**.

A new icon is now in the Network and Dial-Up Connections folder. To use this dial-up connection, double-click the icon in the folder.

Preparing a Windows XP management station for OOB

Before configuring the management station, you must first install the modem. If the modem is already installed, go to the instructions for configuring the dial-up connection.

Install the modem

1 Click **Start** ⇒ **Control Panel** ⇒ **Phone and Modem Options**.

2 Click the **Modems** tab.

3 Click **Add**.
The Add Hardware Wizard appears.

4 Follow the wizard through, completing the information requested.
You will need to know the name and model of the Firebox modem and the modem speed.

5 Click **Finish** to complete the modem installation.

Configure the dial-up connection

1 Click **Start** ⇒ **Control Panel**. Click **Network Connections**. Click **New Connection Wizard**.
The New Connection Wizard appears.

2 Click **Next**. Select **Connect to the network at my workplace**. Click **Next**.

3 Click **Dialup connection**. Click **Next**.

4 Enter a name for your connection.
This can be anything that reminds you of the icon's purpose—OOB Connection, for example.

5 Enter the telephone number of the line connected to the modem in the Firebox. Click **Next**.

6 Click **Finish**.

7 Click either **Dial** or **Cancel**.

A new icon is now in the Network Connections folder. To use this dial-up connection, double-click the icon in the folder.

Configuring the Firebox for OOB

OOB management features are configured in Policy Manager using the **Network Configuration** dialog box, **OOB** tab. The **OOB** tab is divided into two identical halves: the top half controls the settings of any external modem attached; the lower half configures any PCMCIA modem if one is present.

The OOB management features are enabled by default on the Firebox. When trying to connect to a Firebox by way of OOB for the first time, the Firebox first tries to do so with the default settings. From Policy Manager:

1 Select **Network** ⇒ **Configuration**. Click the **OOB** tab.

2 Modify OOB properties according to your security policy preferences. Click **OK**.
For a description of each control, right-click it, and then select What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

Establishing an OOB Connection

From the management station, command your dial-up networking software to call the Firebox modem. After the modems connect, the Firebox negotiates a PPP connection with the calling host, and IP traffic can pass. After the connection is established, you can use System Manager by specifying the dial-up PPP address of the Firebox. The default address is 192.168.254.1.

Configuring PPP for connecting to a Firebox

In its default configuration, Firebox PPP accepts connections from any standard client. The settings you use on your management station are the same as if you were dialing into a typical Internet service provider, except that you need not specify a username or password; leave these fields blank.

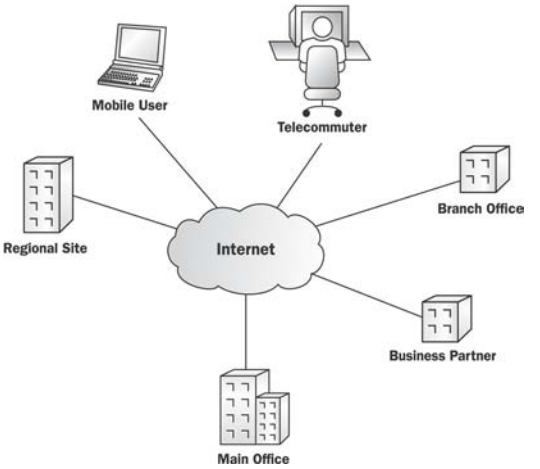
OOB time-out disconnects

The Firebox starts the PPP session and waits for a valid connection from Policy Manager on your management station. If none is received within the default period of 90 seconds, the Firebox terminates the PPP session.

CHAPTER 17

Introduction to VPN Technology

The Internet is a technical development that puts a multitude of information at your fingertips. On this worldwide system of networks, a user at one computer can get information from any other computer. The benefits of using the Internet to exchange data and conduct business are enormous. Unfortunately, so are the risks. Because data packets traveling the Internet are transported in plain text, potentially anyone can read them and place the security of your network in jeopardy.



Virtual private networking technology counters this threat by using the Internet's vast capabilities while reducing its security risk. A virtual private network (VPN) allows communication to flow across the Internet between two networks or between a host and a network in a secure manner. The networks and hosts at the endpoints of a VPN are typically corporate headquarters, branch offices, remote users, telecommuters, and traveling employees. User authentication verifies the identity of both the sender and the receiver. Data sent by way of the Internet is encrypted such that only the sender and the receiver of the message can see it in a clearly readable state.

For more information on VPN technology, see the online support resources at http://www.watchguard.com/support. The main page contains links to basic FAQs, advanced FAQs, and the WatchGuard User's Forum.

Tunneling Protocols

Tunneling—the foundation of VPN implementations—is the transmission of private data through a public network, generally the Internet. Tunneling involves encrypting and encapsulating data and protocol information within units called IP packets. The "tunnel" is the path that the IP packets travel over the Internet. A tunnel is also defined by its start and end points, the type of authentication and encryption used, and the users allowed to use it.

Tunneling protocols provide the infrastructure of virtual private networking. These sets of rules govern how data transmission occurs. Two tunneling protocols widely in use today are Internet Protocol Security (IPSec) and Point-to-Point-Tunneling Protocol (PPTP).

IPSec

The Internet Engineering Task Force (IETF) developed the IPSec protocol suite as a security mechanism to ensure the confidentiality and authenticity of IP packets. IPSec functionality is based on modern cryptographic technologies, providing extremely strong data authentication and privacy. IPSec makes secure

communication possible over the Internet, and IPSec standards allow interoperability between VPN solutions.

A major benefit of IPSec is its interoperability. Instead of specifying a proprietary method for performing authentication and encryption, it works with many systems and standards.

IPSec includes two protocols to deal with issues of data integrity and confidentiality when securing data across the Internet. The AH (Authentication Header) protocol handles data integrity, and the ESP (Encapsulated Security Payload) protocol solves both data integrity and confidentiality issues.

PPTP

PPTP is a widely accepted networking technology that supports VPNs, allowing remote users to access corporate networks securely across the Microsoft Windows operating systems and other point-to-point protocol (PPP)–enabled systems. Although PPTP is not as secure as IPSec, it provides a low-cost, private connection to a corporate network that is easy to implement.

Encryption

In general, intruders can intercept transmitted packets in a network fairly easily and read their contents. VPNs use encryption to keep data confidential as it passes over the Internet to the authorized recipient.

Encryption level is determined by the length of the encryption key. The longer the key, the stronger the encryption level, and the greater the measure of security provided. The level of encryption used in a particular instance depends on the performance and security requirements of the tunnel. Stronger encryption provides a greater level of security but impacts performance. For general-purpose tunnels, over which no sensitive data is to be passed, base encryption provides adequate security with good throughput. For administrative and transactional connections, where exposure of data carries a high risk, strong encryption is recommended.

Within a VPN, after the end points on a tunnel agree upon an encryption scheme, the tunnel initiator encrypts the packet and encapsulates it in an IP packet. The tunnel terminator recovers

the packet, removes the IP information, and then decrypts the packet.

Authentication

An important aspect of security for a VPN is confirming the identity of all communicating parties. Two ways of ensuring identity are password authentication (also called shared secrets) and digital certificates. A shared secret is a passphrase or password that is the same on both ends of a tunnel. The data is encrypted using a session key, which is derived from the shared secret. The gateways can encrypt and decrypt the data correctly only if they share the same secret. Digital certificates use public key–based cyptography to provide identification and authentication of end gateways.

For more information on certificates, see Chapter 19, "Activating the Certificate Authority on the Firebox."

In addition to identifying the user, authentication also defines the resources a user can access. A user must present specified credentials before being allowed access to certain locations on the network.

Extended authentication

Authentication can either take place through a firewall or through an external authentication server such as Remote Authentication Dial-In User Service (RADIUS). An authentication server is a trusted third party that provides authentication services to other systems on a network.

Internet Key Exchange (IKE)

As the number of VPN tunnels between Fireboxes and other IPSec-compliant devices grow, maintaining the large number of session keys used by tunnels becomes a challenge. Keys must also change frequently to ensure the security of each VPN connection.

Internet Key Exchange (IKE)—the key management protocol used with IPSec—automates the process of negotiating and changing keys. IKE implements a security protocol called Inter-

net Security Association and Key Management Protocol (ISAKMP), which uses a two-phase process for establishing an IPSec tunnel. During Phase 1, two gateways establish a secure, authenticated channel for communication. Phase 2 involves an exchange of keys to determine how the data between the two will be encrypted.

Diffie-Hellman is an algorithm used in IKE to negotiate keys required for data encryption. Diffie-Hellman groups are collections of parameters used to achieve the negotiation. These groups allow two peer systems that have no prior knowledge of one another to publicly exchange and agree on a shared secret key. Group 1 is a 768-bit prime modulus group, and group 2 is a 1024-bit prime modulus group—the difference is in the number of bits used for exponentiation to generate private and public keys. Group 2 is more secure than group 1, but requires more time to compute the keys.

WatchGuard VPN Solutions

WatchGuard System Manager offers several methods to provide secure tunnels:

- Mobile User VPN
- Remote User VPN with PPTP
- Branch Office VPN with Basic DVCP
- Branch Office VPN with Manual IPSec
- IPSec tunneling with VPN Manager

NOTE

The last three methods are not supported on Firebox 500 unless you purchase the BOVPN Upgrade. BOVPN is supported on Firebox X700, Firebox X1000, and Firebox X2500 only if you register the device with LiveSecurity Service. To upgrade the Firebox 500 to support BOVPN, see "Enabling the BOVPN Upgrade" on page 317.

WatchGuard offers three different levels of encryption: base, medium, and strong. Base encryption uses a 56-bit encryption key for the Data Encryption Service (DES) algorithm to encrypt

data. Medium encryption uses a 112-bit key for TripleDES, and strong encryption uses a 168-bit key for TripleDES.

Mobile User VPN

NOTE

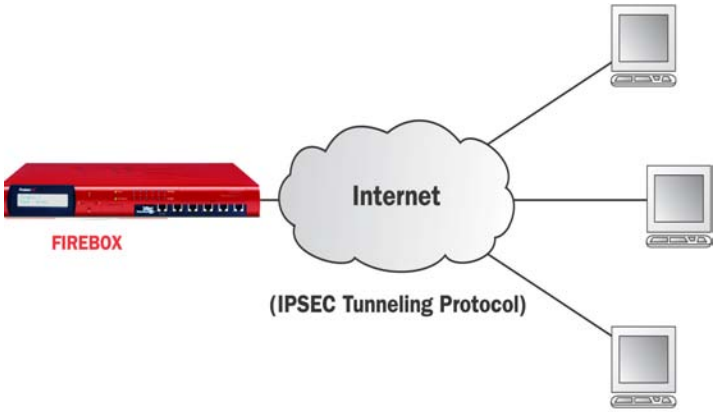
For information on configuring and using MUVPN, see the MUVPN Administrator Guide.

Telecommuters working from home and traveling employees who need corporate network access are common fixtures in today's business environment. Mobile User VPN (MUVPN) creates an IPSec tunnel between an unsecured remote host and your networks using a standard Internet dial-up or broadband connection without compromising security. This type of VPN requires only one Firebox for the private network and the Mobile User VPN software module, which is an optional feature of WatchGuard System Manager.

MUVPN uses IPSec with DES or 3DES-CBC to encrypt incoming traffic and MD5 or SHA-1 to authenticate data packets. You create a security policy configuration and distribute it along with the MUVPN software to each telecommuter. After the software is installed on the telecom-muters' computers, they have a secure way to access corporate resources. MUVPN users can modify their security policy, or you can restrict them such that they have read-only access to the policy.

Certificate-based authentication is supported for MUVPN tunnels. This functionality requires that you configure a Firebox as a DVCP server. DVCP is described in "BOVPN with Basic DVCP" on page 255.

Mobile User VPN is available on all Firebox models including the SOHO 6. Firebox 1000 and 2500 each include a five-user license, and the Firebox 4500 includes a 20-user license. Additional licenses can be added in 5-, 20-, 50-, and 100-pack increments. Large enterprise site licenses are also available.



MUVPN tunnels

MUVPN with extended authentication

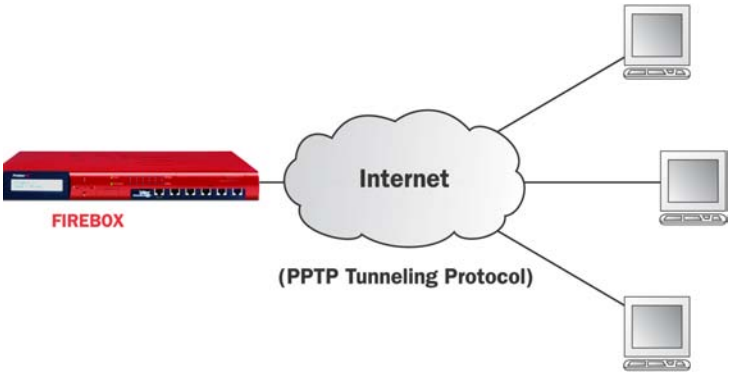
Using MUVPN with extended authentication, users can authenticate to a Windows NT or RADIUS authentication server. Instead of validating against its own data, the Firebox validates users against the third-party server. No usernames or passwords need to be configured on the Firebox.

The advantage of MUVPN with extended authentication is that the network administrator does not have to continually synchronize user login information between the Firebox and the authentication server. MUVPN users log into the corporate network from remote locations using the same username and password they use when they are at their desks inside the company.

RUVPN with PPTP

Remote User VPN (RUVPN) fulfills the same purpose as MUVPN by allowing a remote user to connect to the main office by way of the Internet. However, RUVPN provides a way for telecommuters or travelling employees to connect to the Firebox trusted network using PPTP instead of IPSec.

RUVPN with PPTP is included with the basic WatchGuard System Manager package. It supports up to 50 concurrent sessions per Firebox and works with any Firebox encryption level.



RUVPN with PPTP tunnels

RUVPN with extended authentication

Using RUVPN with extended authentication, users can authenticate to a RADIUS authentication server. Instead of validating against its own data, the Firebox validates users against the third-party authentication server instead. No usernames or passwords need to be loaded onto the Firebox.

Branch Office Virtual Private Network (BOVPN)

NOTE

BOVPN is not supported on Firebox 500 unless you purchase the BOVPN Upgrade. BOVPN is supported on Firebox X700, Firebox X1000, and Firebox X2500 only if you register the device with LiveSecurity Service. To upgrade the Firebox 500 to support BOVPN, see "Enabling the BOVPN Upgrade" on page 317.

Many companies have geographically separated offices that must pass data to one another or access a common database. For example, in a retail chain, each location may need to check inventory in the same centrally located warehouse.

Because branch office communications involve sensitive company data, secure exchange of information is particularly important. Using WatchGuard Branch Office VPN (BOVPN), you can connect two or more locations over the Internet while still protecting the resources of your networks. WatchGuard BOVPN creates a secure tunnel between two networks protected by

WatchGuard System Manager or between a Firebox and another IPSec-compliant device.

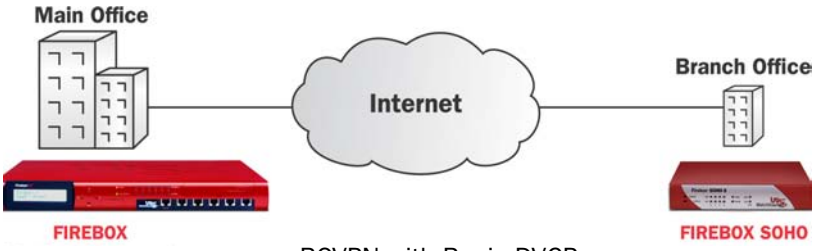
Certificate-based authentication is supported for BOVPN tunnels. This functionality requires that you configure a Firebox as a DVCP server and a certificate authority, as described in the next section and in Chapter 19, “Activating the Certificate Authority on the Firebox.”

BOVPN with Basic DVCP

Dynamic VPN Configuration Protocol (DVCP) is a WatchGuard client server embedded in every WatchGuard Firebox. DVCP simplifies the creation of IPSec tunnels and keeps the user from creating unworkable configurations.

The primary mode of DVCP—Basic DVCP—is used to establish secure IPSec tunnels between Fireboxes and SOHO 6 devices. (Standard DVCP establishes tunnels between devices in VPN Manager, as described in “IPSec tunnels with VPN Manager” on page 256.)

BOVPN with Basic DVCP requires that you define a Firebox as a DVCP server. This server sits at the center of a distributed array of DVCP clients—SOHO 6 devices and SOHO 6|Telecommuters. The DVCP server maintains the connections between two devices by storing all policy information—including network address range and tunnel properties such as encryption, timeouts, and authentication. DVCP clients can retrieve this information from the server. The only information clients need to maintain is an identification name, shared key, and the IP address of the server’s external interface. The DVCP server must have a public IP address.



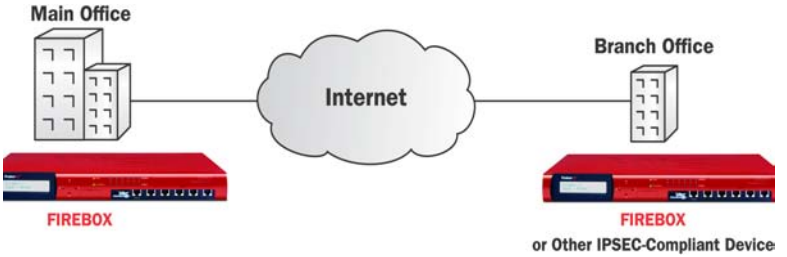
BOVPN with Basic DVCP

BOVPN with Manual IPSec

This BOVPN method uses IPSec to establish encrypted tunnels between a Firebox and any other IPSec-compliant security device, regardless of brand, that may be in service protecting branch office, trading partner, or supplier locations. BOVPN with IPSec is available with the WatchGuard medium encryption version at DES (56-bit) strength, and with the WatchGuard strong encryption versions at both DES (56-bit) and TripleDES (168-bit) strengths.

For manual IPSec, both devices must have a public static IP address.

A main advantage of BOVPN with manual IPSec is that you can order and prioritize routing policies to specify which VPN tunnel to use for certain traffic. For example, you can use DES encryption for VPN traffic originating from your sales team, and the stronger TripleDES encryption for all data transmitted from your finance department.

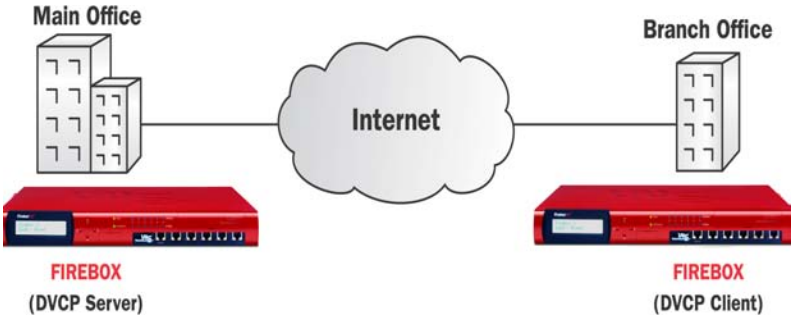


BOVPN with Manual IPSec

IPSec tunnels with VPN Manager

With VPN Manager, you create fully authenticated and encrypted IPSec tunnels using a simple drag-and-drop or menu interface. VPN Manager uses DVCP to securely transmit IPSec VPN configuration information between Fireboxes. Using DVCP, administrators define each configuration aspect of the VPN—such as encryption algorithms and how often encryption keys are negotiated—and then store these settings on a centrally located DVCP server. When a Firebox is installed and initialized, a software client on the Firebox contacts the DVCP server to obtain IPSec policy information.

Using VPN Manager, you can simultaneously configure, manage, and monitor all of the WatchGuard appliances throughout the enterprise. The software eliminates the need for Internet security expertise among branch offices and remote users. Instead, remote users simply plug in the appliance and the administrator at the headquarters does all the rest. If certificates are used for tunnel authentication, all you need to do is configure the Firebox as a certificate authority. The details of certificate generation and distribution are automatically managed by DVCP.



BOVPN with VPN Manager

CHAPTER 18

Designing a VPN Environment

VPN tunnels introduce an additional layer of complexity to the security aspects of your network. When you set up a VPN environment, you are expanding your security perimeter to vulnerable settings such as hotel rooms, airports, and employees' homes. And your company's network security is only as strong as its weakest link.

Another primary concern when deploying VPNs, which must often be balanced with security concerns, is performance. Many of the most secure options available for VPNs come at a high performance cost.

Selecting an Authentication Method

A primary element of a VPN is its method of user authentication. You can use either shared keys or digital certificates to authenticate VPN users. Shared secrets are passwords that must be provided to users. They offer an easy way to quickly set up VPNs to a small number of remote employees, although large numbers of passwords are difficult to manage. To maintain as much security as possible using this method:

- Users should choose strong passwords.
- Passwords should be aged quickly.

- Users should be locked out after three failed login attempts.

When using RUVPN with PPTP or MUVPN, it is especially important to use strong passwords. Compromising the security of VPN endpoints could jeopardize the security of the main network. If, for example, a traveling employee's laptop were stolen, a thief who was able to crack the password would have instant access to the corporate network.

Digital certificates are electronic documents that prove a user's identity. (For a detailed discussion of certificates, see "Public Key Cryptography and Digital Certificates" on page 272.) Certificates are managed by a trusted third party called a certificate authority (CA). In WatchGuard System Manager, a Firebox can be configured to function as a CA. This method of authentication is more secure and scalable than shared secrets.

Selecting an Encryption and Data Integrity Method

Consider both security and performance when choosing encryption and data integrity methods. Out of the two types of encryption supported—DES and TripleDES—the strongest is TripleDES, which is recommended for any sensitive data. Although DES requires less computing time for encryption and decryption, it is recommended only where strong security is not necessary or where use of strong encryption is prevented by export restrictions.

Data integrity ensures that the data received by a VPN endpoint has not been altered while in transit. Two types of data authentication are supported: 128-bit strength Message Digest 5 (MD5-HMAC) and 160-bit strength secure hash algorithm (SHA-HMAC). Because SHA-HMAC has a greater bit strength, it is considered more secure to a small degree, although it may place a slightly heavier load on the processor. However, both MD5 and SHA are considered secure and are used extensively.

IP Addressing

Proper IP addressing is important when creating a VPN. To maintain routing, branch offices should use a unique subnet at

each location. Maintaining different subnets makes management easy and prevents problems in the future if you decide to expand your network.

For MUVPN and RUVPN tunnels, the safest method is to define a "placeholder" secondary network, define a range of addresses for it, and choose an IP address from that network range. This allows you to draw from a range of addresses that do not clash with real host addresses in use behind the Firebox. Using this method, you must also configure the client computer to use the default gateway on the remote host. For information on IP addressing with PPTP tunnels, see the following FAQ: https://www.watchguard.com/support/AdvancedFaqs/pptp_usedgonremote.asp

NAT and VPNs

Implementing an IPSec VPN with a NAT device between remote gateways can require some adjustments. By definition, NAT changes an IP packet's address information. The packet will then fail its data integrity check under the AH protocol, which requires that every bit in the datagram remain unchanged. When using NAT within a tunnel created using BOVPN with Manual IPSec, you must make sure you specify ESP as an authentication method instead of AH. (With all other types of IPSec tunnels, ESP is always used as the authentication method.)

When the Firebox is the NAT device, use IPSec and PPTP passthrough, as described in "Making Outbound IPSec Connections From Behind a Firebox" on page 75 and "Making Outbound PPTP Connections From Behind a Firebox" on page 295.

Access Control

VPNs allow users with varying degrees of trust to access corporate resources. Consider which type of access is appropriate for a given type of user. For example, you might have a group of contract employees you want to restrict to just one network while granting your sales force access to all networks.

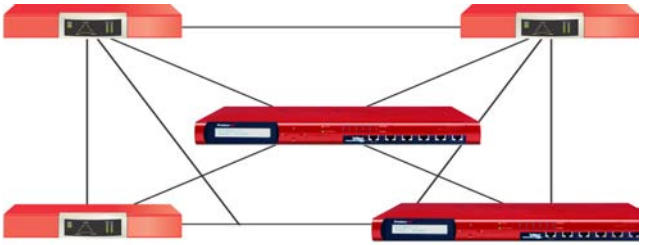
Different VPN applications may also determine your level of trust. Branch office VPNs, because they have a firewall device at both ends of the tunnel, are more secure than MUVPN and RUVPN, which are protected at only one end.

Network Topology

You can configure the VPN to support both meshed and hub-and-spoke configurations. The topology you select determines the types and number of connections that are established, the flow of data, and the flow of routing traffic.

Meshed networks

In a fully meshed topology, as shown in the following figure, all servers are interconnected to form a web, or mesh, with only one hop to any VPN member. Communication can occur between every member of the VPN, whether required or not.



Fully meshed network

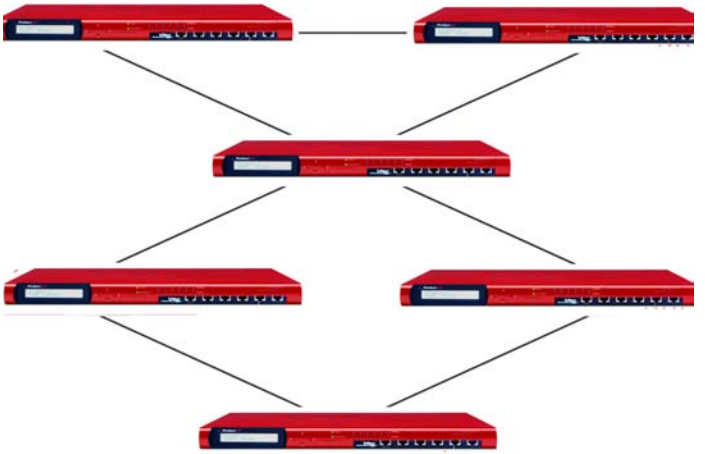
This topology is the most fault-tolerant. If a VPN member goes down, only the connection to that member's protected network is lost. However, this topology has more routing traffic because each VPN member must send updates to every other member. Also, routing loops in a mesh topology can require a significant amount of time to be resolved.

The security of the system as a whole can be maintained and monitored from multiple locations, each deploying a large scale Firebox. This configuration is used by larger enterprises with substantial branch offices, each requiring the higher capacity firewall. Smaller offices and remote users are connected using MUVPN, RUVPN, or SOHO 6 devices.

The main issue with fully meshed networks is scalability. Because every device in the network must communicate with every other device, the number of tunnels required quickly becomes immense. Maintaining such a large number of tunnels can also have a considerable impact on performance. The following equation shows the number of tunnels required for this configuration:

```
[(number of devices)2 = number of tunnels]
```

Partially meshed networks, as shown in the following figure, have only the inter-spoke communications they need and are therefore more scalable than fully meshed networks. A limiting factor in all meshed networks is the number of tunnels that can be supported without overloading the CPU.



Partially meshed network

Hub-and-spoke networks

In a hub-and-spoke configuration, as shown in the following figure, all VPN tunnels terminate at one end of a centrally located and managed firewall appliance. This configuration is frequently used by smaller enterprises with a central Firebox and many distributed remote users connecting with MUVPN, RUVPN, or SOHO 6 devices.

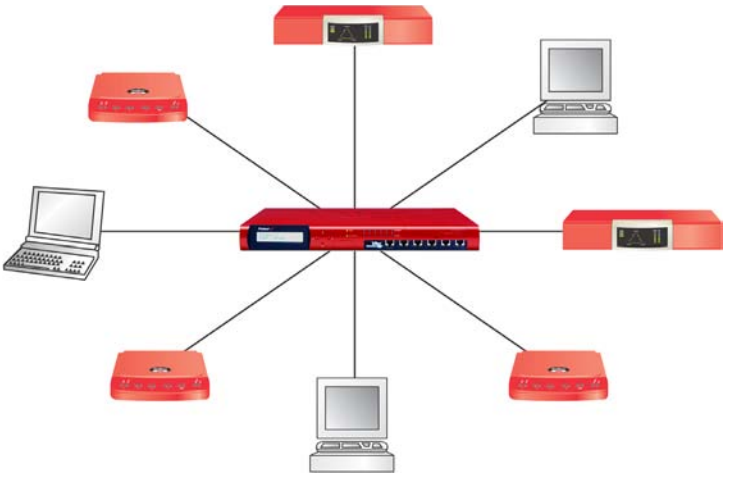
The master server is the central hub of this topology, with all communications radiating outward to other servers and returning to the master server.

In terms of routing traffic, hub-and-spoke is the least traffic-intensive topology, but the master server is the single point of failure. If the master server goes down, an encrypted tunnel cannot be established to any slave server and the ability to send encrypted data to all protected networks is lost.

Hub-and-spoke is far more scalable than meshed with a much more manageable number of tunnels, as shown in the following equation:

```
[(number of devices) – 1 = number of tunnels]
```

The hub site can be expanded as spoke capacity requirements increase. However, because all traffic travels through the hub, this setup requires considerable bandwidth.



Hub-and-spoke network

Tunneling Methods

Split tunneling refers to a remote user or site accessing the Internet on the same machine as the VPN connection but without placing the Internet traffic inside the tunnel. Browsing the Web occurs directly through the user's ISP. This exposes the sys-

tem to attack because the Internet traf-fic is not filtered or encrypted.

The exposure is lessened when all remote users' Internet traffic is routed through VPN to the Firebox, and then back out to the Internet (tunnel switching). Using this configuration allows the Firebox's secure application proxies to inspect traffic that would otherwise go uninspected. This configuration provides a security advantage by reducing the potential for attack.

When using tunnel switching, a NAT policy must cover the outgoing traffic from the remote network to prevent Internet connections from failing.

NOTE

Tunnel switching is not supported from a Firebox to a SOHO 5.

Split tunneling offers a performance advantage at the expense of security. When split tunneling is not allowed or supported, Internet-bound traffic must pass across the WAN bandwidth of the headend twice, which effectively cute connection throughput in half. If you decide to use split tunneling, remote users should have personal firewalls for machines residing on and behind the VPN endpoint.

Determining Which WatchGuard VPN Solution to Use

The five different WatchGuard VPN solutions are each designed for particular applications and setups.

Use BOVPN with Basic DVCP if:

- You are creating tunnels between a Firebox at your main office and dynamically addressed SOHO 6 devices at your branch offices.
- The branch offices do not need to communicate with each other.
- You need only very simple tunnels.

Use BOVPN with Manual IPSec if:

- You are creating tunnels between a Firebox and a non-WatchGuard, IPSec-compliant device.

- You want to assign different routing policies to different tunnels.
- You want to restrict the type of traffic that passes through the tunnel.
- Both devices have a public static address.

NOTE

BOVPN is not supported on Firebox 500 unless you purchase the BOVPN Upgrade. BOVPN is supported on Firebox X700, Firebox X1000, and Firebox X2500 only if you register the device with LiveSecurity Service. To upgrade the Firebox 500 to support BOVPN, see "Enabling the BOVPN Upgrade" on page 317.

Use IPSec tunnels with VPN Manager if:

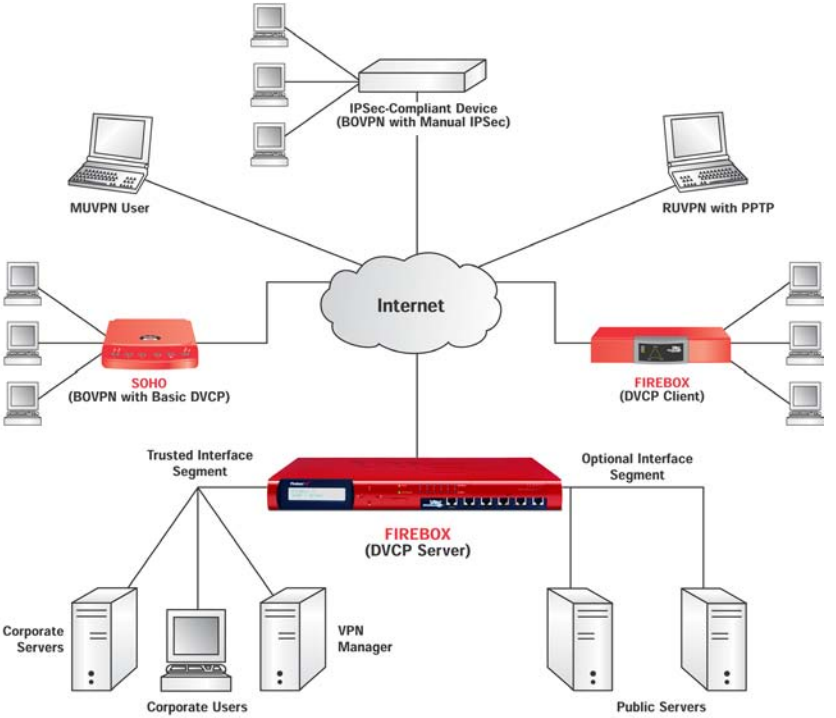
- You are creating tunnels between two or more Fireboxes.
- You want to assign different routing policies to different tunnels.
- Participating client devices are dynamically addressed.
- You have a large number of tunnels to set up.

Use MUVPN if:

- You have mobile users who need to connect securely to a Firebox or SOHO 6.

Use RUVPN with PPTP if:

- You have mobile users who want to connect to the Firebox using PPTP.



WatchGuard VPN Solutions

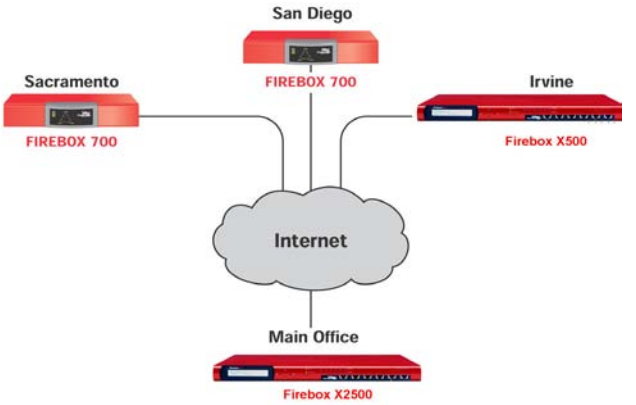
VPN Installation Services

WatchGuard Remote VPN Installation Services are designed to provide you with comprehensive assistance for basic VPN installation, at extra cost. You can schedule a dedicated two-hour time slot with one of our WatchGuard technicians to review your VPN policy, help you configure, and test your VPN configuration. This service assumes you have already properly installed and configured your Fireboxes.

VPN Scenarios

This section describes four different types of enterprises and the VPN solutions that best fit each one.

Large company with branch offices: VPN Manager



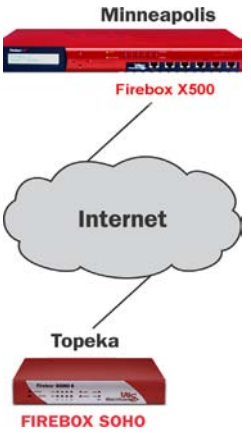
Gallatin Corporation has a main office with about 300 users in Los Angeles and branch offices of around 100 users each in Sacramento, San Diego, and Irvine. All locations have high-speed Internet access, and employees at all locations need secure connections to all other locations.

This enterprise uses Fireboxes at each location and VPN Manager to connect the locations to each other. Each office connects to all other offices, and all users at each office have access to the shared files at all the other locations. The Firebox at headquarters is the DVCP server and the Fireboxes at the branch offices are DVCP clients. Service interruptions occasionally occur with Gallatin's Internet service provider, which renders the Firebox at headquarters unavailable, but the tunnels among the other locations remain in place.

Medium-sized company with main office and auxiliary office: BOVPN with Basic DVCP

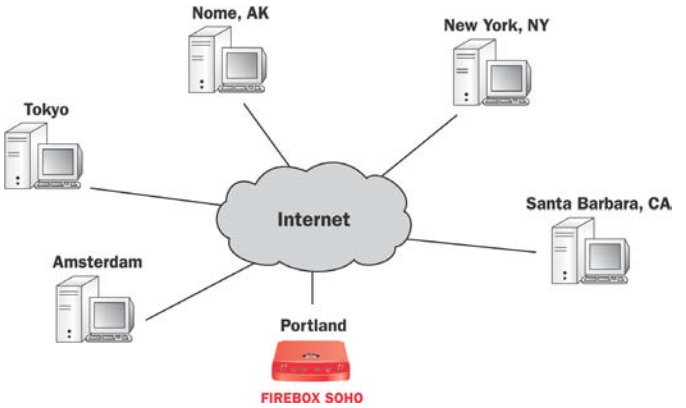
Arrington's Plumbing Supply has a main office in Minneapolis, Minnesota and a distribution center in Topeka, Kansas. The main office has a Firebox 700 on a T1 connection and the distribution center has a SOHO 6|tc. The two offices have secure access to one another using Basic DVCP, which allows the SOHO 6 to establish a VPN with the Firebox despite the SOHO 6 device's public IP address changing from time to time. The eight

employees at the distribution center can access all shared files at headquarters, and headquarters can access the inventory computers in Topeka.



Small company with telecommuters: MUVPN

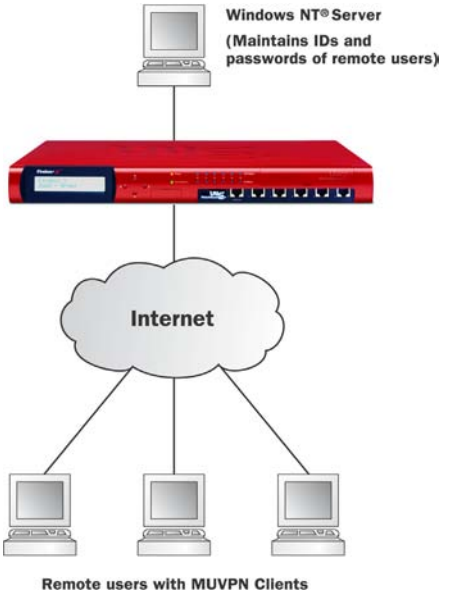
River Rock Press is a small publishing house serving a speciality market. It has an office with six employees in Portland, Oregon and five editors who live all over the world. The main office uses a SOHO 6 for firewalling and as a VPN gateway, and the five editors each use a Mobile User VPN client to securely connect to the River Rock Information Center in Portland. The editors are able to securely exchange information any time their computers are connected to the Internet.



Company with remote employees: MUVPN with extended authentication

BizMentors, Inc employs 35 trainers to deliver courses in business-related topics at client companies' facilities. BizMentor's 75 salespeople need up-to-the minute information on the trainers' schedules to avoid scheduling conflicts. This information is kept current on a database located in BizMentors' data center. The data center uses a Firebox, and each salesperson uses an MUVPN client to access the inventory and price database. A Windows NT server at the data center is used to authenticate all remote users.

Normally, the ID and password information must be entered and maintained on both the Firebox and the Windows NT server. However, using extended authentication, all IDs and passwords are validated against the Windows NT server and do not need to be loaded onto the Firebox. All salespersons can log into the corporate network with the ID and password they normally use when inside the network. The Firebox validates the ID and password against the Windows NT server instead of its own internal data.



CHAPTER 19

Activating the Certificate Authority on the Firebox

All WatchGuard tunnels created using IPSec can be authenticated using either shared secrets or *digital certificates*. A certificate is an electronic document containing a public key which provides proof that the key belongs to a legitimate party and has not been compromised. Certificates are issued to clients by a trusted third party called a certificate authority (CA). In WatchGuard System Manager, a Firebox that is configured as a DVCP server also functions as a CA.

Certificates provide a stronger and more scalable means of authentication than shared secrets. Although many CAs in the marketplace are complex to deploy, the WatchGuard CA is easily configured and performs authentication functions with minimal input required by the user.

CAs are part of a system of key generation, key management, and certification called a Public Key Infrastructure (PKI). The PKI provides for certificate and directory services that can generate, distribute, store, and—when necessary, revoke the certificates.

Public Key Cryptography and Digital Certificates

A central fixture of a PKI is an information protection method called *public key cryptography.* This cryptographic system involves two mathematically related keys, known as a key pair. One key, the private key, is kept secret by the owner of the key. The other key, known as the public key, may be distributed far and wide by its owner. The keys in the key pair are complementary. Only the private key can decrypt information encrypted with the public key. And only the public key verifies information signed with the private key.

The integrity and identity of public keys is maintained using digital certificates. A root certificate, which contains the public key of the CA, ensures that the client certificates are valid.

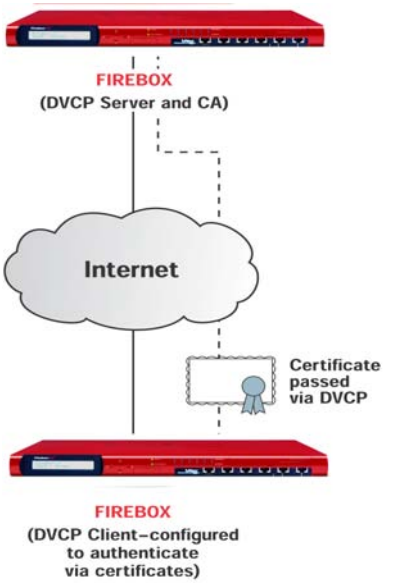
Certificates have a fixed lifetime that is determined when they are issued. However, certificates are sometimes revoked before the expiration date and time that was originally set for them. To keep track of which certificates are no longer valid, the CA maintains an online, up-to-date listing of revoked certificates called a certificate revocation list (CRL). Before validating a certificate, the CRL is checked to make sure the certificate has not been revoked.

PKI in a WatchGuard VPN

For authenticating by way of certificates, the Firebox must be configured as a DVCP server, which automatically activates the CA on the Firebox. Each DVCP client authenticates to the DVCP server. The CA determines that the client is legitimate and then returns a certificate to the client.

The CA can be configured in several ways. A common structure, shown in the following figure, includes a Firebox as a DVCP server that is managing a DVCP client. The DVCP server can also manage a number of DVCP clients known as a DVCP cluster. The CA component of the DVCP server is active regardless of whether either Firebox authenticates through certificates. The authentication method is determined by settings in the DVCP clients. In the following example, one DVCP client authenticates

using certificates. When the client contacts the server, the CA downloads a certificate to the Firebox using DVCP.

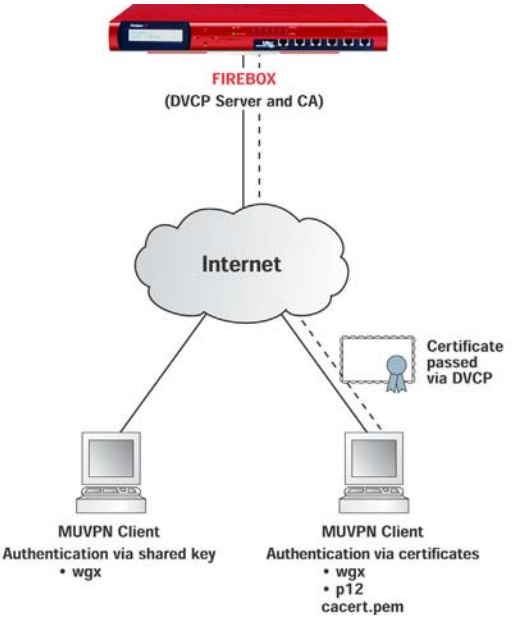


DVCP server/CA with DVCP client

The following figure shows a Firebox that is not part of a DVCP cluster. Instead, the Firebox functions as a CA for MUVPN users. In this example, one MUVPN user is authenticating through certificates and the other by shared key. Because MUVPN clients are not DVCP clients, they authenticate to the Firebox, and WatchGuard System Manager creates a request for a certificate. After the CA issues the certificate, System Manager packages the certificate for transport to the MUVPN client.

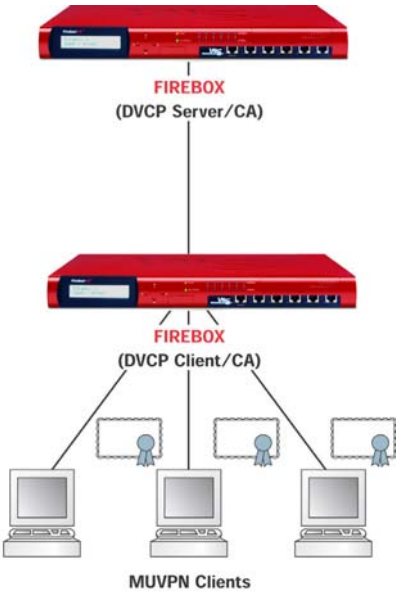
The Firebox administrator provides each MUVPN user with a collection of settings called an MUVPN end-user profile. Users who are authenticating with shared keys receive one file, `.wgx`. Users authenticating with certificates receive a `.wgx` file along with two other files: `cacert.pem`, which contains the root certificate; and `.p12`, the client certificate. When the MUVPN user authenticating by way of certificates opens the `.wgx` file,

the root and client certificates contained in the `cacert.pem` and `.p12` files are automatically loaded.



DVCP server/CA with MUVPN clients

Another configuration, shown in the following figure, involves a DVCP server/CA at a company's main office and a Firebox as a DVCP client at a branch office. The branch office supports mobile users authenticating by way of certificates. This scenario comprises two CAs—a principal CA and a subordinate one.



DVCP server/CA, DVCP client/CA, and MUVPN clients

Defining a Firebox as a DVCP Server and CA

When you designate a Firebox as a DVCP server, you also enable it as a certificate authority. You can configure a DVCP server from either Policy Manager or VPN Manager.

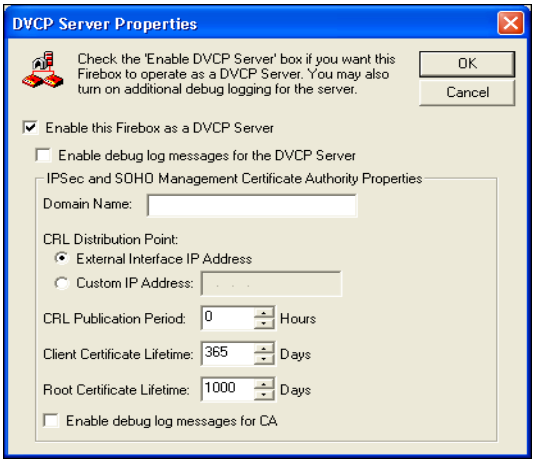
NOTE

Only a Firebox with a static IP address can be defined as a DVCP server.

Using Policy Manager

1 Open System Manager and connect to the Firebox you want to define as a DVCP server.
The Firebox must have its name set using Setup ⇒Name for the CA to function properly.

2 From Policy Manager, select **Network ⇒DVCP Server**.
The DVCP Server Properties window appears, as shown in the following figure.


DVCP Server Properties
Check the 'Enable DVCP Server' box if you want this Firebox to operate as a DVCP Server. You may also turn on additional debug logging for the server.
OK
Cancel
Enable this Firebox as a DVCP Server
Enable debug log messages for the DVCP Server
IPSec and SOHO Management Certificate Authority Properties
Domain Name:
CRL Distribution Point:
External Interface IP Address
Custom IP Address:
CRL Publication Period:
0
Hours
Client Certificate Lifetime:
365
Days
Root Certificate Lifetime:
1000
Days
Enable debug log messages for CA

3 Select the **Enable this Firebox as a DVCP Server** checkbox.

4 If you want to enable debug logging for the server, select the **Enable Debug Log Messages for the DVCP Server** checkbox.

5 Enter the domain name for the IPSec and SOHO Management Certificate Authority Properties.

6 Select the Certificate Revocation List (CRL) end point.
This is either an external interface IP address or custom IP address.

7 Enter the CRL Publication period in hours.
This is the period of time a particular CRL is available.

8 Enter the client certificate lifetime in days.

9 Enter the root (CA) certificate lifetime in days.

10 Select the box **Enable debug log messages for CA** to have these messages sent to the WSEP log host.

NOTE

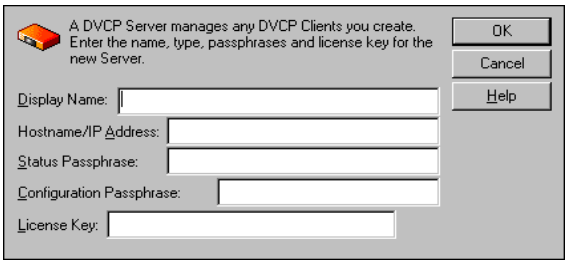
Make sure you set CA properties correctly. Changing CA properties after initial setup will invalidate all certificates.

11 Click **OK**.

12 From Policy Manager, select **File ⇒Save ⇒To Firebox**, create or verify the name for the configuration file, and enter the Firebox's read-write passphrase.

Using VPN Manager

1 Open VPN Manager and select **File ⇒ New**.
The New Server dialog box appears.



2 Enter the following:

Display Name
A friendly name of your choosing. This becomes the name of the Firebox acting as the DVCP server.

Host Name or IP Address
This is either the device's DNS name or its external IP address.

Status Pass Phrase
This is the current status (read-only) passphrase.

Configuration Pass Phrase
This is the current configuration (read/write) passphrase. This is also the passphrase used when configuring a device that is inserted into VPN Manager.

License Key
The key listed on your VPN Manager License Key Certificate.

3 Click **OK**.
A message appears confirming the DVCP server setup.

4 Click **OK**.
The Firebox reboots. It is now activated as a DVCP server.

NOTE

If you are configuring BOVPN tunnels using certificates for authentication, you must use the WatchGuard Security Event Processor (WSEP) for logging. Because certificates use timestamps, all devices in a VPN using certificates for authentication must be using the same timekeeping method.

Managing the Certificate Authority

You can manage various aspects of the certificate authority on the Firebox using the Web-based CA manager.

1 After activating the CA on the Firebox, access the Web-based Certificate Authority Settings pages. You can do this from several locations:
   - From the System Manager Main Menu, select **Tools** ⇒ **Advanced** ⇒ **CA Manager**.
   - From VPN Manager, select **Resources** ⇒ **CA Manager**.
   - From VPN Manager, click the CA Manager icon (shown at right).



   VPN Manager and System Manager must first be connected to the Firebox designated as a DVCP server.

2 Enter the Firebox configuration passphrase when prompted.
   The main menu of the Certificate Authority Settings pages appears.

3 From the main menu, select the page you want as follows:

Generate a New Certificate

Enter a subject common name, organizational unit, password, and certificate lifetime to generate a new certificate.
   - For MUVPN users, the common name should match the username of the remote user.
   - For Firebox users, the common name should match the Firebox identifier (normally, its IP address).
   - For a generic certificate, the common name is the name of the user.

NOTE

Enter the organizational unit specification only if you are generating certificates for MUVPN users. It is not used with other types of VPN tunnels. The unit name should appear in the following format:
GW:<*vpn gateway name*>
where <*vpn gateway name*> is the value of config.watchguard.id in the gateway Firebox's configuration file.

Publish a Certificate Revocation List (CRL)
Force the CA to publish the CRL to all certificate-holding clients.

Publish the CA Certificate
Print a copy of the CA (root) certificate to the screen so you can manually save it to the client.

Find and Manage Certificates
Specify the serial number, subject common name, or subject organizational unit of a certificate to be located in the database. Also, instead of a particular certificate, you can specify that only valid, revoked, or expired certificates are located. The results of the search are displayed on the List Certificates page, as described below.

List and Manage Certificates
View a list of certificates currently in the database and select certificates to be published, revoked, reinstated, or destroyed. For information on performing these actions on certificates, see the next section.

Upload CA Credentials
Use this page to force the certificate authority on a particular Firebox to become subordinate to the master CA. The master CA will generate a private key and certificate for the Firebox. Enter the name of the credentials file containing the key and certificate (or click Browse to locate it) to be uploaded to the Firebox.

Upload Certificate Request
Use this page to import a certificate request from a third party. Specify the subject common name and organizational unit. Enter or browse to locate the certificate signing request file.

Managing certificates from the CA Manager

You use the List and Manage Certificates page to publish, revoke, reinstate, or destroy certificates:

1 From the List and Manage Certificates page, click the serial number of the certificate on which you want to perform the action.
The certificate data appears.

2 From the **Choose Action** drop-down list, select from the following choices and then click **GO**:

Publish (PEM)
Publishes the certificate in Privacy Enhanced Mail (PEM) format, which uses a protocol to provide secure Internet mail. This option allows you to save the certificate to a file and upload it to a third-party device.

Publish (PKC12)
Publishes the certificate in PKCS12 format, which is used by most Web browsers. This option allows you to save the certificate to a file and upload it to a third-party device.

Revoke
Revokes a certificate. This action does not publish a CRL.

Reinstate
Reinstates a previously revoked certificate.

Destroy
Destroys a certificate.

Restarting the CA

When the CA root certificate expires, you must restart the CA to force it to reissue a new root certificate.

From System Manager:

1 Click the Main Menu button (shown at right). Select **Management ⇒ Restart CA**.



2 When asked to confirm, click **Yes**.

3 Enter the Firebox configuration (read/write) passphrase.

4 When prompted, click **Yes**.

CHAPTER 20

Configuring RUVPN with PPTP

Remote User Virtual Private Networking (RUVPN) uses Point-to-Point Tunneling Protocol (PPTP) to establish a secure connection between an unsecured remote host and a protected network. It supports up to 50 concurrent sessions per Firebox and works with any Firebox encryption level. RUVPN requires configuration of both the Firebox and the end-user remote host computers.

RUVPN users can authenticate either to the Firebox or to a RADIUS authentication server.

Configuration Checklist

Before configuring a Firebox to use RUVPN, gather this information:

- The IP addresses to assign to the remote client during RUVPN sessions. **These IP addresses cannot be addresses that are currently used in the network.** The safest way to allocate addresses for RUVPN users is to define a "placeholder" secondary network, define a range of addresses for it, and choose an IP address from that network range. For example, define an unused subnet as a secondary network on your trusted network 10.10.0.254/

24 and define 10.10.0.0/27 for your pool of PPTP addresses. For more information, see “IP Addressing” on page 260.

- The IP addresses of the DNS and WINS servers in the trusted network that perform IP address lookup on host alias names.
- The usernames and passwords of those authorized to connect to the Firebox using RUVPN.

Encryption levels

Because of strict export restrictions placed on exported high encryption software, WatchGuard Firebox products are packaged with base encryption on the installation CD.

For RUVPN with PPTP, you can select to use 128-bit encryption or 40-bit encryption. U.S. domestic versions of Windows XP ship with 128-bit encryption enabled by default, but earlier versions of Windows may require a strong encryption patch, available from Microsoft. The Firebox always attempts to negotiate 128-bit encryption first, and drops down (if enabled) to 40-bit if the client is unable to negotiate the 128-bit encrypted connection. For information on how to enable the drop to 40-bit, see “Activating RUVPN with PPTP” on page 287. For more information on encryption levels and PPTP tunnels, see the following FAQ: https://www.watchguard.com/support/AdvancedFaqs/pptp_tunnelencryp.asp

If you live outside the U.S. and you need to activate strong encryption on your LiveSecurity Service account, send an email to supportid@watchguard.com and include in the request:

- Your active LiveSecurity Service key number
- Date purchased
- The name of your company
- Mailing address
- Telephone contact number and name
- Email address to respond to

If you live in the U.S., you must download the strong encryption software from your archive page in the LiveSecurity Service Web site. Go to www.watchguard.com, click **Support**, log into

your LiveSecurity Service account, and then click **Latest Software**.

After you have downloaded or activated the strong encryption software, uninstall the original encryption software, and then install the strong encryption software from the downloaded file.

NOTE

If you want to retain your current Firebox configuration when performing the uninstall/reinstall, do not set up the Firebox with the QuickSetup Wizard when reinstalling. Instead, open System Manager, connect to the Firebox, and save the current configuration file. Configurations generated with any encryption version are compatible.

Configuring WINS and DNS Servers

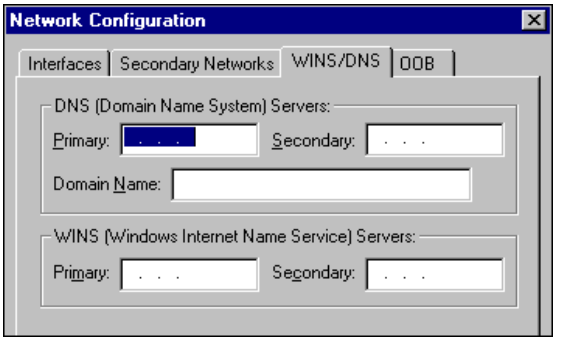
RUVPN clients rely on shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS translates host names into IP addresses, while WINS resolves NetBIOS names to IP addresses. These servers must be accessible from the Firebox trusted interface.

Make sure you use only an internal DNS server. Do not use external DNS servers.

From Policy Manager:

1 Select **Network** ⇒ **Configuration**. Click the **WINS/DNS** tab.
The information for the WINS and DNS servers appears, as shown in the following figure.

2 Enter primary and secondary addresses for the WINS and DNS servers. Enter a domain name for the DNS server.



Adding New Users to Authentication Groups

All RUVPN users must be placed in a built-in Firebox authentication group called pptp_users. This group, which contains the usernames and passwords of RUVPN users, is used to configure the allowed services for incoming traffic, as described in the next section.

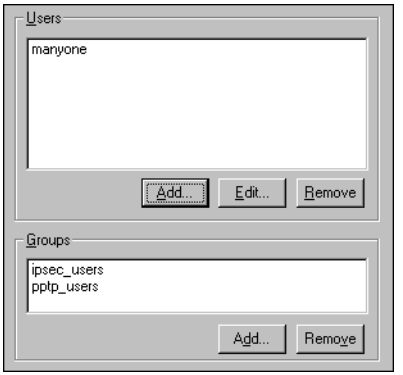
To gain access to Internet services (such as outgoing HTTP or outgoing FTP), the remote user provides authenticating data in the form of a username and password, and the WatchGuard System Manager software authenticates the user to the Firebox.

For more information on Firebox groups, see Chapter 10, "Creating Aliases and Implementing Authentication."

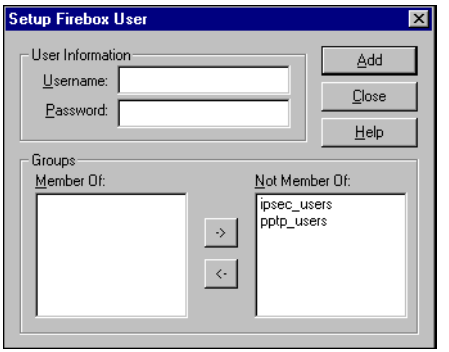
From Policy Manager:

1 Select **Setup ⇒ Authentication Servers**.
The Authentication Servers dialog box appears.

2 Click the **Firebox Users** tab.
The information on the tab appears as shown in the following figure.



3 To add a new user, click the **Add** button beneath the **Users** list.
The Setup Firebox User dialog box appears, as shown below.



4 Enter a username and password for the new user.

5 Select **pptp_users** in the **Not Member Of** list, and then click the left-pointing arrow to move the name to the **Member Of** list. Click **Add**.

The user is added to the User list. The Setup Remote User dialog box remains open and cleared for entry of another user.

6 To close the **Setup Remote User** dialog box after you have finished adding new users, click **Close**.

The Firebox Users tab appears with a list of the newly configured users.

7 When you finish adding all users you want to add, click **OK**.

The users and groups can now be used to configure services, as explained in the next section.

Configuring Services to Allow Incoming RUVPN Traffic

By default, RUVPN users have no access privileges through a Firebox. To allow remote users to access machines behind the Firebox (on the trusted network, for example), you must either add their individual user names or the entire pptp_users group to service icons in the Services Arena.

WatchGuard recommends two methods for configuring services for RUVPN traffic: by individual service and by using the Any service. Configuring the Any service “opens a hole” through the Firebox, allowing all traffic to flow unfiltered between specific hosts.

By individual service

In the Services Arena, double-click a service that you want to enable for your VPN users. Set the following properties on the service:

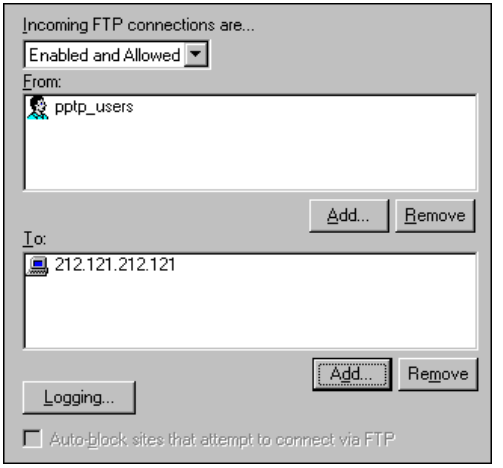
Incoming

- Enabled and allowed
- From: pptp_users
- To: trusted, optional, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: trusted, optional, network or host IP address, or alias
- To: pptp_users

An example of how you might define incoming properties for a service appears on the following figure.



Using the Any service

Add the Any service with the following properties:

Incoming

- Enabled and allowed
- From: pptp_users

- To: trusted, optional, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: trusted, optional, network or host IP address, or alias
- To: pptp_users

Make sure you save your configuration file to the Firebox after making these changes.

NOTE

If you want to use WebBlocker to control remote users' Web access, add pptp_users to whichever proxy service controls WebBlocker (such as Proxied-HTTP) instead of the Any service.

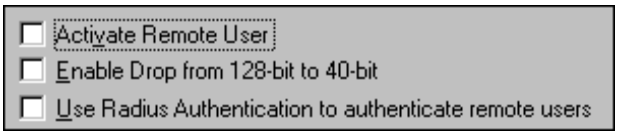
Activating RUVPN with PPTP

The next step in configuring RUVPN with PPTP is activating the feature. Activating RUVPN with PPTP adds the wg_pptp service icon to the Services Arena, which sets default properties for PPTP connections and the traffic flowing to and from them. The wg_pptp service rarely requires modification, and WatchGuard recommends leaving it in its default settings. From Policy Manager:

1 Select **Network ⇒ Remote User**. Click the **PPTP** tab.

2 Select the checkbox marked **Activate Remote User**.

3 If necessary, select the checkbox marked **Enable Drop from 128-bit to 40-bit**.
In general, this checkbox is used only by international customers.



Enabling Extended Authentication

RUVPN with extended authentication allows users to authenticate to a RADIUS authentication server instead of to the Firebox. For more information on extended authentication, see “Extended authentication” on page 250.

1 Select the checkbox marked **Use RADIUS Authentication to authenticate remote users,** as shown in the previous figure.

2 Configure the RADIUS server using the **Authentication Servers** dialog box, as described in Chapter 10, “Creating Aliases and Implementing Authentication.”

3 On the RADIUS server, add the user to the pptp_users group.

Entering IP Addresses for RUVPN Sessions

RUVPN with PPTP supports 50 concurrent sessions, although you can configure a virtually unlimited number of client computers. The Firebox dynamically assigns an open IP address to each incoming RUVPN session from a pool of available addresses until this number is reached. After the user closes a session, the address reverts to the available pool and is assigned to the next user who logs in.

For more information on assigning IP addresses to RUVPN clients, see “IP Addressing” on page 260.

From the **PPTP** tab on the **Remote User Setup** dialog box:

1 Click **Add**.
The Add Address dialog box, as shown below, appears.



2 Use the **Choose Type** drop-down list to select either a host or network.

You can configure up to 50 addresses. If you select a network address, RUVPN with PPTP will use the first 50 addresses in the subnet.

3 In the **Value** field, enter the host or network address in slash notation. Click **OK**.

Enter unused IP addresses that the Firebox can dynamically assign to clients during RUVPN with PPTP sessions. The IP address appears in the list of addresses available to remote clients.

4 Repeat the add process until all addresses for use with RUVPN with PPTP are configured.

Configuring Debugging Options

WatchGuard offers a selection of logging options you can set to gather information and help with future troubleshooting. Because enabling these debugging options can significantly increase log message volume and have potentially adverse impacts on Firebox performance, it is recommended that they be enabled only for troubleshooting RUVPN problems.

1 From Policy Manager, click **Network ⇒ Remote User VPN**.

The Remote User Setup window appears with the Mobile User VPN tab selected.

2 Click the **PPTP** tab.

3 Click **Logging**.

The PPTP Logging dialog box appears.

4 Click the logging options you want to activate.

For a description of each option, right-click it, and then click What's This?. You can also refer to the "Field Definitions" chapter in the Reference Guide.

5 Click **OK**. Save the configuration file to the Firebox.

Preparing the Client Computers

Every computer used as an RUVPN with PPTP remote host must first be prepared with the following:

- Operating system software
- Device drivers

- Internet service provider (ISP) account
- Public IP address

After you have obtained these basic requirements, follow the procedures in this section to perform the following:

- Install the required version of Microsoft Dial-Up Networking and any required service packs
- Prepare the operating system for VPN connections
- Install a VPN adapter (not required for all operating systems)

Installing MSDUN and Service Packs

The client computer may need MSDUN (Microsoft Dial-Up Networking) upgrades installed and other extensions and service packs for proper configuration. Currently, RUVPN with PPTP requires these upgrades according to platform:

Encryption	Platform	Application
Base	Windows NT	40-bit SP4
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2

*40-bit encryption is the default for Windows 2000. If you are upgrading from Windows 98, in which you had set strong encryption, Windows 2000 will automatically define strong encryption for the new installation.

To install these upgrades or service packs, go to the Microsoft Download Center Web site at:
http://www.microsoft.com/downloads/search.asp

Windows NT Platform Preparation

To prepare a Windows NT remote host, you must specify PPTP as your protocol, choose the number of VPNs, and set up remote access.

From the Windows NT Desktop of the client computer:

1 Click **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click **Network**.

2 Click the **Protocols** tab.

3 Click **Add**.

4 Select **Point To Point Tunneling Protocol**.

5 Choose the number of VPNs.
Unless a separate host will be connecting to this machine, you need only one VPN.

6 In the **Remote Access Setup** box, click **Add**.

7 Select **VPN** on the left. Select **VPN2-RASPPTPM** on the right.

8 Click **Configure** for the newly added device.

9 Click **Dial Out Only**. Click **Continue**.

10 Click **OK**.

11 Restart the machine.

Adding a domain name to a Windows NT workstation

Often, remote clients need to connect to a domain behind the firewall. To do this, the remote client must recognize the domains to which they belong. Adding a domain requires the installation of the Computer Browser Network Service. From the Windows NT Desktop:

To install a Computer Browser Service

1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click **Network**.
The Network dialog box appears.

2 Click the **Services** tab.

3 Click **Add**.

4 Select **Computer Browser**.

5 Browse to locate the installation directory. Click **OK**.

6 Restart the workstation.

To add a new domain

1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click **Network**.
The Network dialog box appears.

2 Click the **Protocols** tab.

3 Select **Computer Browser**. Click **Properties**.

4 Add the remote network domain name.
You can add multiple domain names during the same configuration session.

5 Click **OK**.

6 Reboot the workstation.

Installing a VPN adapter on Windows NT

In addition to basic platform preparation, RUVPN with PPTP requires the installation and configuration of a VPN adapter.

From the Windows NT Desktop of the remote host:

1 Double-click **My Computer**.

2 Double-click **Dial-Up Networking**.
If you have not already configured an entry, Windows guides you through the creation of a dial-up configuration. When it prompts for a phone number, enter the host name or IP address of the Firebox. When complete, you should see a Dial-Up Networking dialog box with the default button Dial.

3 Select **New** to make a new connection. If you are prompted to use the wizard, enter a friendly connection name and select the **I Know All About** checkbox.

4 Under the **Basic** tab, configure the following settings:
- **Phone Number**: Firebox IP address
- **Entry Name**: Connect to RUVPN (or your preferred alternative)
- **Dial Using**: RASPPTPM (VPN1) adapter
- **Use Another Port if Busy**: enabled

5 Click the **Server** tab. Configure the following settings:
- **PPP**: Windows NT, Windows 95 Plus, Internet
- **TCP/IP**: enabled
- **Enable Software Compression**: enabled

6 Click the **Security** tab. Configure the following settings:
- **Accept Only Microsoft Encrypted Authentication**: enabled
- **Require Data Encryption**: enabled

7 Click **OK**.

Windows 2000 Platform Preparation

To prepare a Windows 2000 remote host, you must configure the network connection.

From the Windows Desktop of the client computer:

1. Select **Start ⇒ Settings ⇒ Dial-Up Network and Connections ⇒ Make New Connection**.
   The Network Connection wizard appears.
2. Click **Next**.
3. Select **Connect to a private network through the Internet**. Click **Next**.
4. Enter the host name or IP address of the Firebox external interface. Click **Next**.
5. Select whether the connection is for all users or only the currently logged-on user. Click **Next**.
6. Enter a name you want to use for the new connection, such as "Connect with RUVPN." Click **Finish**.

Windows XP Platform Preparation

To prepare a Windows XP remote host, you must configure the network connection. (Because the PPTP functionality is built into Windows XP, you do not need to install a VPN adapter as you would for the Windows NT platform.)

From the Windows Desktop of the client computer:

1. Select **Start ⇒ Control Panel ⇒ Network and Internet Connections**.
   The Network Connection wizard appears.
2. Click **Next**.
3. Select **Connect to the network at my workplace**. Click **Next**.
4. Select **Virtual Private Connection**. Click **Next**.
5. Enter a name you want to use for the new connection, such as "Connect with RUVPN." Click **Next**.
6. Select **Automatically dial this initial connection**. Click **Next**.

7 Enter the host name or IP address of the Firebox external interface. Click **Next**.

8 Click **Finish**.

Starting RUVPN with PPTP

The connect process is identical regardless of the Windows platform you are using. From the Windows Desktop:

1 Establish an Internet connection through either Dial-Up Networking or directly through a LAN or WAN.

2 Double-click **My Computer**. Double-click **Dial-Up Networking**.

3 Double-click the dial-up networking connection you made for your PPTP connection to the Firebox.

4 Enter the remote client username and password.
These were assigned when you added the user to the pptp_users group, as described in "Adding New Users to Authentication Groups" on page 284.

5 Click **Connect**.

Running RUVPN and Accessing the Internet

You can enable remote users to access the Internet through a RUVPN tunnel. However, this option has certain security implications, as described in "Network Topology" on page 262.

1 When you are setting up your connection on the client computer, select the **Use default gateway on remote network** checkbox. In Windows NT, this checkbox is located on the **TCP/IP Settings** dialog box. In Windows 2000 and Windows XP, it is located on the **Advanced TCP/IP Settings** dialog box.

2 On the Firebox, create a dynamic NAT entry from VPN to external. If you want to specify that only certain PPTP users have this ability, create entries from <virtual IP address> to External.

3 Configure your Outgoing service to allow outgoing connections from pptp_users to the external interface.

However, if you want to use WebBlocker to control remote users' Web access, add pptp_users to whichever proxy service controls WebBlocker (such as Proxied-HTTP) instead of the Outgoing service.

Making Outbound PPTP Connections From Behind a Firebox

You may have occasions in which a user wants to make PPTP connections to a Firebox from behind another Firebox. For example, if a mobile employee travels to a customer site that has a Firebox, he or she can make PPTP connections to his or her network using PPTP. For the local Firebox to properly handle the outgoing PPTP connection, a PPTP service must be set up as follows:

1 Add the PPTP service. (For information on enabling services, see Chapter 8, "Configuring Filtered Services.")

2 Select **Setup** ⇒ **NAT**, and make sure the checkbox marked **Enable Dynamic NAT** is selected. This is the default for a Firebox in routed mode.

Making Outbound IPSec Connections From Behind a Firebox

1 Add the IPSec service. (For information on enabling services, see Chapter 8, "Configuring Filtered Services.")

2 On both the **Incoming** and **Outgoing** tabs, select **Enabled and Allowed**.

3 Select **Setup** ⇒ **NAT**, and make sure the checkbox marked **Enable Dynamic NAT** is selected. This is the default for a Firebox in routed mode.

The Any to Any configuration of the IPSec packet filter is not a security risk in routed mode; only the external IP will answer IPSec incoming requests. If you are using drop-in mode, it will open these ports for all public computers; howrever, IPSec is a secure protocol. You can restrict the incoming of IPSec connections when you add this service, but be sure not to conflict with

allowing IPSec traffic to reach the Firebox external IP for BOVPN traffic you have configured.

CHAPTER 21

Configuring BOVPN with Basic DVCP

Dynamic VPN Configuration Protocol (DVCP) is the WatchGuard-proprietary protocol that easily creates IPSec tunnels. The type of DVCP described in this chapter is known as Basic DVCP, which can establish VPN tunnels between devices in a hub-and-spoke formation.

The Basic DVCP server is a Firebox that sits at the center of a distributed array of DVCP clients. This server maintains the connections between two devices by storing all policy information—including network address range and tunnel properties such as encryption, timeouts, and authentication. DVCP clients can retrieve this information from the server. The only information clients need to maintain is an identification name, shared key, and the IP address of the server's external interface.

You use the DVCP Client Wizard to configure a Firebox as a DVCP server and create tunnels to each client device. The clients then contact the server and automatically download the information needed for them to connect securely.

NOTE

BOVPN is not supported on Firebox 500 unless you purchase the BOVPN Upgrade. BOVPN is supported on Firebox X700, Firebox X1000, and Firebox X2500 only if you register the device with LiveSecurity Service. To upgrade the Firebox 500 to support BOVPN, see "Enabling the BOVPN Upgrade" on page 317.

Configuration Checklist

Before implementing BOVPN with DVCP, gather the following information:

- IP address of the Firebox that will act as the Basic DVCP server (must be a static public address).
- IP network addresses for the networks communicating with one another.
- A common passphrase, known as a shared secret.

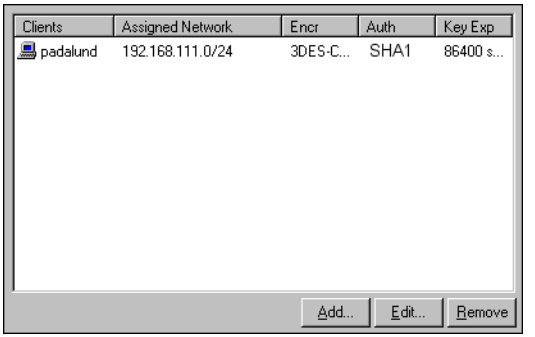
Creating a Tunnel to a Device

Use the following procedure to create a tunnel to a device.

The tunnels you create to SOHO 6 clients must be completely distinct from any tunnel created for branch office VPN, regardless of whether they are being managed through DVCP or manually (as described in the next chapter). The networks on the trusted side of the SOHO cannot be the same as any other SOHO device's trusted network (unless you are using a Telecommuter tunnel).

From Policy Manager:

1 Select **Network ⇒ Branch Office VPN ⇒ Basic DVCP Server**.
The Basic DVCP Server Configuration dialog box appears, showing the clients configured to use DVCP as shown in the following figure.



2 Click **Add**.
The DVCP Client Wizard launches.

3 Enter a distinctive name for the DVCP client.
The client name appears in the Basic DVCP Server Configuration dialog box as well as the Firebox and Tunnel Status display.

4 Enter the shared key that the client and server will use for encryption. Click **Next**.

5 Enter the IP address of the network or host that the DVCP client will be able to access.

6 Select a client type and then enter the virtual network or IP address this client will use for connections. (Note that this IP address or subnet must not conflict with any other SOHO 6 or range on the Firebox.) Click **Next**.

Telecommuter IP Address
The SOHO 6 is assigned a single IP address. This is the device's virtual IP address on the trusted network of the Firebox to which the device will be allowed access.

Private Network
(Recommended) The device is assigned an entire network.

7 Use the **Type** drop-down list to select an encryption type:

ESP (Encapsulated Security Payload)
Performs encryption and/or authentication

AH (Authentication Header)
Performs authentication only

8 Use the **Authentication** drop-down list to select an authentication method:

None
No authentication

MD5-HMAC
128-bit algorithm

SHA1-HMAC (Recommended)
160-bit algorithm

9 If you chose **ESP** in the **Type** drop-down list, see the **Encryption** drop-down list to select an encryption method:

None
No encryption

DES-CBC (Recommended)
56-bit encryption

3DES-CBC
168-bit encryption

10 Enter a key expiration time in kilobytes, hours, or both.
If you specify both, the key expires at whichever time arrives earliest.

11 Click **Next**. Click **Finish**. Save the configuration to the Firebox.

The new policy appears in the **Basic DVCP Server Configuration** dialog box. The WatchGuard device can now be connected, powered on, and configured. As part of the configuration process, it will automatically download the appropriate tunnel information. You must provide the DVCP client administrator with the client name, shared key, and the IP address of the server's external interface.

If you want to add more networks that the DVCP client can access, edit the entry and add the networks.

Editing a tunnel to a device

You can change the following properties of a DVCP tunnel without forcing the client to reboot:

- Identification name
- Shared key
- Encryption/authentication level
- Timeouts

You can also change the network range of a WatchGuard client. However, when you save the configuration to the server, it automatically triggers the client to reboot and load the new policy.

From Policy Manager:

1 Select **Network ⇒ Branch Office VPN ⇒ Basic DVCP Server**.
The Basic DVCP Server Configuration dialog box appears

2 Select the DVCP client you want to edit. Click **Edit**.
The DVCP Client Wizard opens and displays the tunnel properties.

3 Use the **Next** and **Back** buttons to move through the DVCP Client Wizard and reconfigure tunnel properties. When complete, click **Finish**.

4 Save the configuration to the Firebox.
The next time the client contacts the server, it automatically notes the tunnel policy change and downloads the modifications. If the network address range on a client has changed, the client automatically restarts.

Removing a tunnel to a device

When a tunnel is removed, the DVCP client can no longer communicate with the server. The next time the DVCP client tries to contact the server, contact will be denied. If these settings were never manually configured, the client will use 192.168.111.0/24 as the DVCP network range.

From Policy Manager:

1 Select **Network ⇒ Branch Office VPN ⇒ Basic DVCP**.

2 Select the tunnel policy. Click **Remove**.
The policy is removed from the DVCP Configuration dialog box.

Configuring Logging for a DVCP Server

You can set several logging options for IPSec, including:

- Configuration dump after IKE interpretation
- IKE debugging messages
- Trace of IKE packets and their movements
- Certificate validation debugging

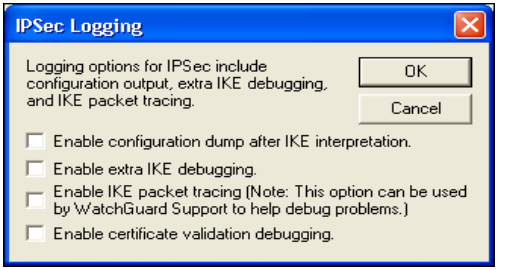
Note, however, that these logging options can generate a high volume of traffic and can affect VPN performance. This is par-

ticularly true of tracing the IKE packets. Enable these options only to troubleshoot problems.

From Policy Manager:

1 Select **Network ⇒ Branch Office VPN ⇒ Basic DVCP**.
The Basic DVCP Server Configuration dialog box appears.

2 Click the **Logging** button at the right of the dialog box.
The IPSec Logging dialog box, as shown below, appears.


IPSec Logging
Logging options for IPSec include configuration output, extra IKE debugging, and IKE packet tracing.
OK
Cancel
Enable configuration dump after IKE interpretation.
Enable extra IKE debugging.
Enable IKE packet tracing (Note: This option can be used by WatchGuard Support to help debug problems.)
Enable certificate validation debugging.

3 Select the checkbox or checkboxes for the logging options you want. Save the configuration to the Firebox.

CHAPTER 22

Configuring BOVPN with Manual IPSec

Branch Office VPN (BOVPN) with Manual IPSec establishes encrypted tunnels between a Firebox and any other IPSec-compliant security device, regardless of brand, that may be in service protecting branch office, trading partner, or supplier locations.

BOVPN with Manual IPSec is available with the WatchGuard medium encryption version at DES (56-bit) strength, and with the WatchGuard strong encryption versions at both DES (56-bit) and TripleDES (168-bit) strengths.

NOTE

BOVPN is not supported on Firebox 500 unless you purchase the BOVPN Upgrade. BOVPN is supported on Firebox X700, Firebox X1000, and Firebox X2500 only if you register the device with LiveSecurity Service. To upgrade the Firebox 500 to support BOVPN, see "Enabling the BOVPN Upgrade" on page 317.

NOTE

Manual IPSec tunnels are not supported to Fireboxes that are configured as DHCP or PPPoE clients (have dynamically assigned external IP addresses). Both devices must have static public IP addresses. Also, Manual IPSec tunnels do not support incoming static NAT.

Configuration Checklist

Before implementing BOVPN with Manual IPSec, gather the following information:

- Public IP address of both ends of the tunnel
- Policy endpoints—IP addresses of specific hosts or networks participating in the tunnel
- Encryption method (both ends of the tunnel must use the same encryption method)
- Authentication method

Configuring a Gateway

A gateway specifies a point of connection for one or more tunnels. The standard specified for a gateway, such as ISAKMP automated key negotiation, becomes the standard for tunnels created with the device at the other end of the tunnel.

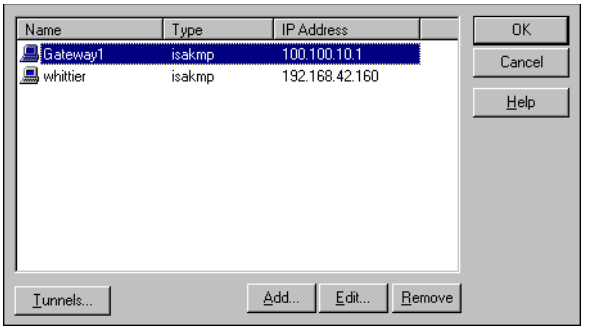
Adding a gateway

For an IPSec tunnel negotiation to begin, at least one peer must be able to contact the other. This can be done using an IP address or a DNS name. If the peer is dynamic, an IP address cannot be used. However, if the peer has dynamic DNS capabilities, the Firebox can be configured to perform a DNS resolution on the peer's identity. The resolution turns the DNS name into an IP address so the negotiation can begin. To configure, set the remote gateway's ID type to **Domain Name** and the peer's identity to the fully qualified domain name. Set the Firebox's DNS server to one which can resolve the name, usually an internal DNS server.

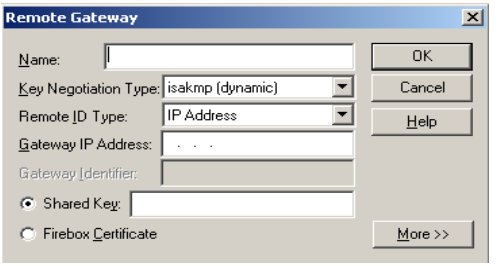
From Policy Manager:

1 Select **Network ⇒ Branch Office VPN ⇒ Manual IPSec**.
The IPSec Configuration dialog box appears. The Manual IPSec menu option is disabled if you have a Firebox 500 and have not purchased the BOVPN Upgrade.

2 Click **Gateways**.
The Configure Gateways dialog box appears, as shown in the following figure.



3 To add a gateway, click **Add**.
The Remote Gateway dialog box appears, as shown below.



4 Enter the gateway name.
This name identifies a gateway only within Policy Manager.

5 Use the **Key Negotiation Type** drop-down list to select either **ISAKMP (dynamic)** or **Manual**.

6 Use the **Remote ID Type** drop-down list to select either IP Address, Domain Name, or User Name.
The Firebox uses IP Address and Domain Name to locate the VPN endpoint. User name is simply a label you apply to designate the user at the VPN endpoint.

NOTE

For VPNs using WatchGuard devices, WatchGuard recommends using the default value of IP Address in the Remote ID Type field. If this value needs to be changed for interoperability, consult the appropriate interoperability document for information on the values you should use in this field.

7 Enter the gateway IP address or identifier according to your previous selection.

A SOHO using DHCP or PPPoE for its external IP address must use the domain name as the identifier in the Firebox configuration.

8 Select either the Shared Key or Firebox Certificate option to specify the authentication method to be used. If you select Shared Key, enter the shared key.

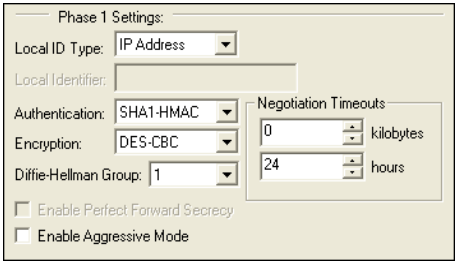
These options are available only for ISAKMP-negotiated gateways. The same key must be entered at the remote device.

NOTE

If you choose to authenticate using certificates, the certificate authority must be active on the Firebox. For information on activating the CA, see Chapter 19, "Activating the Certificate Authority on the Firebox." In addition, if you use certificates, you must use the WatchGuard Security Event Processor for logging.

9 If you want to define Phase 1 settings, click **More**.

The Phase 1 settings fields appear, as shown in the following figure. Phase 1 refers to the initial phase of the IKE negotiation. It involves authentication, session negotiation, and key exchange.



10 In the **Local ID Type** drop-down list, specify IP Address, Domain Name, or User Name.

The Firebox uses IP Address and Domain Name to locate the VPN endpoint. User name is simply a label you apply to designate the user at the VPN endpoint.

NOTE

For VPNs using WatchGuard devices, WatchGuard recommends using the default value in the Local ID Type field, which is the external IP address of the Firebox. If this value needs to be changed for interoperability, consult the appropriate interoperability document for information on the values you should use in this field.

11 In the **Authentication** field, specify the type of authentication: SHA1-HMAC or MD5-HMAC.

12 In the **Encryption field**, enter the type of encryption: DES-CBC or 3DES-CBC.

13 In the **Diffie-Hellman group** field, specify the group. WatchGuard supports groups 1 & 2.

Diffie-Hellman refers to a mathematical technique for securely negotatiating secret keys over a public medium. Diffie-Hellman groups are collections of parameters used to achieve this. Group 2 is more secure than group 1, but requires more time to compute the keys.

14 If you choose, select the checkbox marked **Enable Perfect Forward Secrecy**.

When this option is selected, each new key that is negotiated is derived by a new Diffie-Hellman exchange instead of from only one Diffie-Hellman exchange. Enabling this option provides more security, but requires more time because of the additional exchange.

15 If you choose, select the checkbox marked **Enable Aggressive Mode**.

Mode refers to an exchange of messages in Phase 1. Main Mode is the default.

16 Specify negotiation timeouts in either kilobytes, hours, or both.

If you specify both, the timeout occurs at whichever time arrives earliest.

17 When you finish adding gateways, click **OK** to return to the **IPSec Configuration** dialog box.

Editing and removing a gateway

To edit a gateway, from the **Configure Gateways** dialog box:

1 Select the gateway and click **Edit**.
The Remote Gateway dialog box appears.

2 Make changes according to your security policy preferences and click **OK**.

To remove a gateway, from the **Configure Gateways** dialog box, select the gateway and click **Remove**.

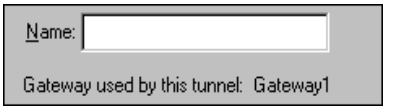
Creating a Tunnel with Manual Security

The following describes how to configure a tunnel using a gateway with the manual key negotiation type. From the **IPSec configuration** dialog box:

1 Click **Tunnels**.
The Configure Tunnels dialog box appears.

2 Click **Add**.
The Select Gateway dialog box appears.

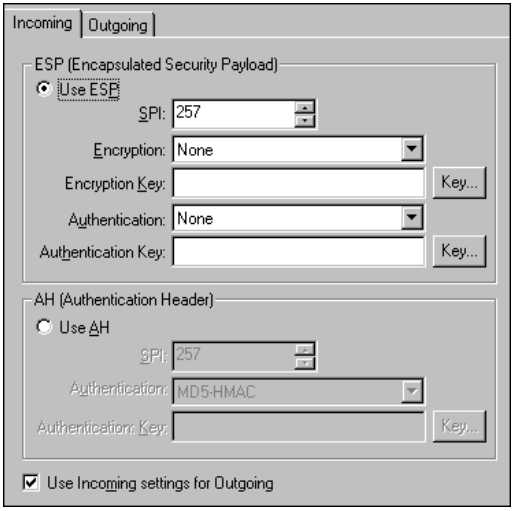
3 Select a remote gateway with manual key negotiation type to associate with this tunnel (the key negotiation type is displayed in the **Type** column at the **Configure Tunnels** dialog box). Click **OK**.
The Identity tab of the Configure Tunnel dialog box appears, as shown in the following figure.



4 Type a tunnel name.
Policy Manager uses the tunnel name as an identifier.

5 Click the **Manual Security** tab. Click **Settings**.
The Incoming tab of the Security Association Setup dialog box appears.

6 Click the **Phase 2 Settings** tab.
The Phase 2 settings fields appear, as shown in the following figure.



7 Click either the ESP or AH security method option. Configure the chosen security method.

The difference between the two is that ESP can provide both authentication and encryption while AH provides authentication only. Also, ESP authentication does not cover the encapsulated IP header while AH does. (AH is rarely used.)
For more information on configuring these security methods, see "Using Encapsulated Security Protocol (ESP)" on page 310 and "Using Authenticated Headers (AH)" on page 310.

8 To use the same settings for both incoming and outgoing traffic, select the **Use Incoming Settings for Outgoing** checkbox.

If you select this checkbox, you are done with the Security Association Setup dialog box and can proceed to the next step. If you clear this checkbox, click the Outgoing tab and configure the security associations for outgoing traffic. The fields have the same rules and parameter ranges as the Incoming tab.

9 Click **OK**.

The Configure Tunnels dialog box appears displaying the newly created tunnel. Repeat the tunnel creation procedure until you have created all tunnels for this particular gateway.

10 After you add all tunnels for this gateway, click **OK**.

The Configure Gateways dialog box appears.

11 To configure more tunnels for another gateway, click **Tunnels**. Select a new gateway and repeat the tunnel creation procedure for that gateway.

12 When all the tunnels are created, click **OK**.

Using Encapsulated Security Protocol (ESP)

1 Type or use the SPI scroll control to identify the Security Parameter Index (SPI).
   You must select a number between 257 and 1023.

2 Use the **Encryption** drop-down list to select an encryption algorithm.
   Options include: None (no encryption), DES-CBC (56-bit), and 3DES-CBC (168-bit).

3 If you selected DES-CBC or 3DES-CBC, click **Key**.

4 Type a passphrase for generating a key. Click **OK**.
   The passphrase appears in the Encryption Key field. You cannot enter a key in that field directly.

5 Use the **Authentication** drop-down list to select an authentication algorithm.
   Options include: None (no authentication), MD5-HMAC (128-bit algorithm), or SHA1-HMAC (160-bit algorithm).

6 If you selected MD5-HMAC or SHA1-HMAC, click **Key**.

7 Type a passphrase for generating a key. Click **OK**.
   The passphrase appears in the Authentication Key field. You cannot enter a key here directly.

Using Authenticated Headers (AH)

1 Type or use the SPI scroll control to identify the Security Parameter Index (SPI).
   You must select a number between 257 and 1023.

2 Use the **Authentication** drop-down list to select an authentication method.
   Options include: MD5-HMAC (128-bit algorithm) or SHA1-HMAC (160-bit algorithm).

3 Click **Key**. Enter a passphrase for generating a key. Click **OK**.
   The passphrase appears in the Authentication Key field. You cannot enter a key here directly.

NOTE

If both ends of the tunnel have Fireboxes, the remote administrator can also enter the encryption and authentication passphrases. If the remote firewall host is an IPSec-compliant device of another manufacturer, the remote system administrator must enter the literal keys displayed in the Security Association Setup dialog box when setting up the remote IPSec-compliant device.

Creating a Tunnel with Dynamic Key Negotiation

The following describes how to configure a tunnel using a gateway with the Internet Security Association and Key Management Protocol (ISAKMP) key negotiation type. ISAKMP is a protocol for authenticating communication between two devices. This process involves defining how the entities will use security services such as encryption, and how to generate the keys that will be used to convert the encrypted data back into plain text.

From the **IPSec Configuration** dialog box:

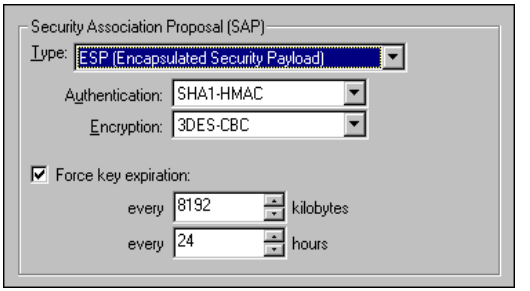
1 Click **Tunnels.**
The Configure Tunnels dialog box appears.

2 Click **Add**.

3 Click a gateway with ISAKMP (dynamic) key negotiation type to associate with this tunnel. Click **OK**.

4 Type a tunnel name.
Policy Manager uses the tunnel name as an identifier.

5 Click the **Phase 2 Settings** tab.
The Phase 2 fields appear, as shown in the following figure.



6 Use the **Type** drop-down list to select a Security Association Proposal (SAP) type.
Options include: Encapsulated Security Payload (ESP) or Authenticated Headers (AH).

7 Use the **Authentication** drop-down list to select an authentication method.
Options include: None (no authentication), MD5-HMAC (128-bit algorithm), and SHA1-HMAC (160-bit authentication algorithm).

8 Use the **Encryption** drop-down list to select an encryption method.
Options include: None (no encryption), DES-CBC (56-bit), and 3DES-CBC (168-bit encryption).

9 To have a new key generated periodically, select the **Force Key Expiration** checkbox.
With this option, transparent to the user, the ISAKMP controller generates and negotiates a new key for the session. For no key expiration, enter 0 (zero) here. If you select the Force Key Expiration checkbox, set the number of kilobytes transferred or hours passed in the session before a new key is generated for continuation of the VPN session.

10 Click **OK**.
The Configure Tunnels dialog box appears displaying the newly created tunnel. Repeat the tunnel creation procedure until you have created all tunnels for this gateway.

11 After you add all tunnels for this gateway, click **OK**.
The Configure Gateways dialog box appears.

12 To configure more tunnels for another gateway, click **Tunnels**. Select a new gateway and repeat the tunnel creation procedure for that gateway.

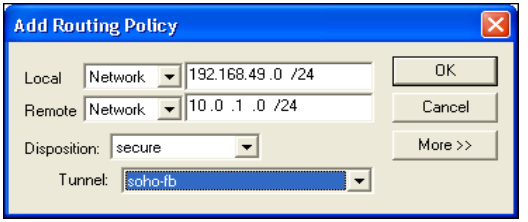
13 When all tunnels are created, click **OK**.

Creating a Routing Policy

Routing policies are sets of rules, much like packet filter rules, for defining how outgoing IPSec packets are built. They also determine whether incoming IPSec packets can be accepted. Policies are defined by their endpoints. These are not the same as tunnel or gateway endpoints—endpoints that define policies are the specific hosts or networks attached to the tunnel's Fireboxes (or other IPSec-compliant devices) that communicate through the tunnel.

From the **IPSec Configuration** dialog box:

1 Click **Add**.
The Add Routing Policy dialog box appears, as shown below.



2 Use the **Local** drop-down list to specify a local host or network.

3 Enter the IP or network address in slash notation for the local host or network.

4 Use the **Remote** drop-down list to select a remote host or network.

5 Enter the IP address or network address in slash notation for the remote host or network.

6 Use the **Disposition** drop-down list to select a bypass rule for the tunnel:

Secure
IPSec encrypts all traffic that matches the rule in associated tunnel policies.

Block
IPSec does not allow traffic that matches the rule in associated tunnel policies.

Bypass
IPSec passes traffic that matches this rule without encryption; that is, this traffic will “bypass” the IPSec routing policy.

NOTE

For every tunnel created to a dropped-in device, you must create a host policy for both sides' external IP addresses that has protection set to Bypass. Otherwise, traffic to and from the dropped-in device's external IP address will conflict with any network policy associated with the VPN. In addition, make sure Bypass policies are at the top of the policy list or move them accordingly, as explained in "Changing IPSec policy order" on page 315.

7 If you chose **Secure** as your disposition, use the **Tunnel** drop-down list to select a configured tunnel.

To configure a new tunnel, see "Creating a Tunnel with Manual Security" on page 308 or "Creating a Tunnel with Dynamic Key Negotiation" on page 311. To display additional information about the selected tunnel, click More.

8 If you want to restrict the policy to a specific source port, destination port, or protocol, click **More**.

The fields for ports and protocol appear, as shown below.



9 To restrict the policy to a single destination port, in the **Dst Port** field, enter the remote host port.

The remote host port number is optional. The port number is the port to which WatchGuard sends communication for the policy. To enable communications to all ports, enter zero (0).

NOTE

WatchGuard recommends that you limit connection ports in Policy Manger, not BOVPN.

10 Use the **Protocol** drop-down list to limit the protocol used by the policy.

Options include: * (specify ports but not protocol), TCP, and UDP.

11 To restrict the policy to a single source port, in the **Src Port** field, enter the local host port.

The local host port number is optional. The port number is the port from which the Firebox sends all communication for the policy. To enable communication from all ports, enter zero (0).

NOTE

If you restrict the policy to a specific source, port, or protocol, you may inadvertantly block legitimate traffic.

12 Click **OK**.
The IPSec Configuration dialog box appears listing the newly created policy. Policies are listed in the order in which they were created. To change the order, see the next section.

Configuring routing policies for proxies over VPN tunnels

Connections from BOVPN tunnels to the Internet, when using a VPN peer as the default route, are considered outgoing connections and can be proxied.

From the **IPSec Configuration** dialog box:

1 Click **Add**.
The Add Routing Policy dialog box appears.
2 In the drop-down list next to **Local**, select **Network**.
3 Set the IP address as 0.0.0.0/0.
4 Use the **Remote** drop-down list to select a remote host or network.
5 Enter the IP address or network address in slash notation for the remote host or network.
6 In the **Disposition** drop-down list, select **Secure**.
7 From Policy Manager, add a proxy service as described in “Adding a service” on page 111.
8 On the **Properties** tab, click **Outgoing**.
9 Under the **From** list, click **Add**.
10 Click **Network IP Address** and use the address you used for **Remote** in step 5.
11 Under the **To** list, click **Add**.
12 In the Members box, double-click **External**.

Changing IPSec policy order

The Firebox handles policies in the order listed, from top to bottom, on the **IPSec Configuration** dialog box. Initially, the policies are listed in the order created. You must manually reorder the policies from more specific to less specific to ensure that

sensitive connections are routed along the higher-security tunnels. In general, WatchGuard recommends the following policy order:

- Host to host
- Host to network
- Network to host
- Network to network

Policies must be set to the same order at both ends of the tunnel.

From the **IPSec Configuration** dialog box:

- To move a policy up in the list, click the policy. Click **Move Up**.
- To move a policy down in the list, click the policy. Click **Move Down**.

Configuring multiple policies per tunnel

If you use two or more policies for a tunnel, the order must be identical on each Firebox. For example, suppose Firebox1 and Firebox2 have a tunnel defined between them and both Fireboxes have Policy A and Policy B. For the tunnel to operate, both Fireboxes must define Policy A followed by Policy B. If, instead, one Firebox has Policy A defined first and the other has Policy B defined first, the tunnel will not operate.

If you have multiple routing policies to a device, each routing policy tunnel must have a unique name. For additional policies, add a new tunnel, and then give it a unique name with the same gateway and security settings. When you add this routing policy, select the second tunnel name.

Configuring services for BOVPN with IPSec

Access control is a critical part of configuring a secure VPN environment. If machines on the branch office VPN network are compromised, attackers can get a secure tunnel to your network.

Users on the remote Firebox are technically outside the trusted network; you must therefore configure the Firebox to allow traffic through the VPN connection. A quick method is to create a host alias corresponding to the VPN remote networks and hosts.

Then, use either the host alias or individually enter the remote VPN networks and hosts when configuring the following service properties:

Incoming

- Enabled and Allowed
- From: Remote VPN network, hosts, or host alias
- To: Trusted or selected hosts

Outgoing

- Enabled and Allowed
- From: Trusted network or selected hosts
- To: Remote VPN network, hosts, or host alias

For more information on configuring services, see Chapter 8, "Configuring Filtered Services."

Allow VPN access to any services

To allow all traffic from VPN connections, add the Any service to the Services Arena and configure it as described previously.

Allow VPN access to selective services

To allow traffic from VPN connections only for specific services, add each service to the Services Arena and configure each as described previously.

Enabling the BOVPN Upgrade

Although the factory default Firebox 500 does not support BOVPN, you can purchase a license key to enable this option. (BOVPN is supported on Firebox 700, Firebox X1000, and Firebox X2500 only if you register the device with LiveSecurity Service.)

Like other WatchGuard System Manager options, the BOVPN Upgrade option is available from your local reseller. For more information about purchasing WatchGuard products, go to: http://www.watchguard.com/sales/

To enable the BOVPN option after you have received your license key:

1 From Policy Manager, select **Setup ⇒Firebox Model**. Make sure **Firebox III/500** or **Firebox X500** is selected.

2 From Policy Manager, select **Network ⇒ Branch Office VPN ⇒ Manual IPSec**.
The IPSec Configuration dialog box appears.

3 Click the **License** button.
The IPSec Branch Office License dialog box appears.

4 Type your license key in the field to the left of the **Add** button. Click **Add**.

CHAPTER 23

Configuring IPSec Tunnels with VPN Manager

WatchGuard VPN Manager offers speed and reliability through drag-and-drop tunnel creation, automatic wizard launching, and the application of templates. With VPN Manager, you create fully authenticated and encrypted IPSec tunnels in minutes, and you can be assured that they do not clash with other tunnels or security policies.

From the same GUI, you can then administer and monitor the tunnels and view the status of the various components and tunnels at a glance. For more information on monitoring tunnels using VPN Manager, see Chapter 24, "Monitoring VPN Devices and Tunnels."

VPN Manager also provides a secure way to remotely manage SOHO 6 devices. For more information, see Chapter 25, "Managing the SOHO 6 with VPN Manager."

NOTE

BOVPN is not supported on Firebox 500 unless you purchase the BOVPN Upgrade. BOVPN is supported on Firebox X700, Firebox X1000, and Firebox X2500 only if you register the device with LiveSecurity Service. You can add a Firebox 500 to VPN Manager as a device, but you cannot create tunnels to it.

To upgrade the Firebox 500 to support BOVPN, see "Enabling the BOVPN Upgrade" on page 317.

Steps in creating VPNs using VPN Manager

To configure VPN Manager you must:

- Designate a Firebox as a DVCP server and Certificate Authority (CA)
- (Dynamic devices only) Add Fireboxes or SOHO 6 devices to the VPN Manager device list
- (Dynamic devices only) Configure the Firebox as a DVCP client
- Build policy templates to designate which networks are accessible through VPN tunnels
- Build security templates to set encryption level and authentication type
- Create tunnels between devices

Defining a Firebox as a DVCP Server and CA

The first step in setting up a VPN tunnel using VPN Manager is defining a Firebox as a DVCP server. This automatically activates the certificate authority on the Firebox, whether you choose to authenticate by way of certificates or shared keys.

For information on defining the Firebox as a DVCP server and CA, see Chapter 19, "Activating the Certificate Authority on the Firebox."

Launching VPN Manager

1 **Start ⇒ Programs ⇒ WatchGuard ⇒ VPN Manager.**

2 When prompted, enter the configuration passphrase of the Firebox functioning as your DVCP server.
The VPN Manager UI appears, as shown in the following figure.



Adding Devices to VPN Manager (Dynamic Devices Only)

If the devices enabled as DVCP clients use dynamic IP addresses, you must manually add them to your VPN configuration. This step is unnecessary if you are using static devices.

NOTE

You can add a factory default Firebox 500 to VPN Manager as a device, but you cannot create tunnels to it. To upgrade the Firebox 500 to support BOVPN, see "Enabling the BOVPN Upgrade" on page 317.

From VPN Manager:

1 Select either the **Device** or the **VPNs** tab. Select **Edit** ⇒ **Insert Device**.
The WatchGuard Device Wizard appears.

2 Click **Next**.

3 Enter a display name for the device.
This is a name of your own choosing. It is not tied to the device's DNS name.

4 From the **Device Type** drop-down list, select **Dynamic SOHO**. The SOHO must have dynamic DNS configured.

5 Enter the unique ID or shared secret.
This is the DNS name, not the name you entered in Step 3.

6 Enter the status and configuration passphrases.

7 If you specified a device type with a dynamic IP address, enter the shared secret. Click **Next**.

8 Specify the default method used to authenticate tunnels with this Firebox: autogenerated shared key or Firebox certificate (RSA signature). Click **Next**.

9 Enter any WINS or DNS server IP addresses you want in your configuration. Click **Next**.
If you are not using DNS or WINS servers, ignore this page, and click Next.
The wizard displays the Contact Information page.

10 Enter any contact information you want for contacting administrators of this Firebox. Click **Next**.
The information on this page is optional.

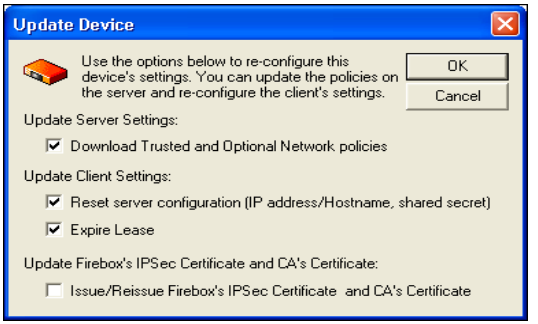
11 The wizard then displays a page describing what the steps will be performed next. Click **Next**.
When finished, the wizard displays the message New Device Successfully Changed.

12 Click **Close**.
The wizard uploads the new configuration to the DVCP server and exits.

Updating a device's settings

You can use the **Update Device** dialog box to reconfigure the settings of a selected device.

1 From the **VPNs** tab, right-click a device and select **Update Device**.
The Update Device dialog box appears, as shown in the following figure.


Update Device
Use the options below to re-configure this device's settings. You can update the policies on the server and re-configure the client's settings.
OK
Cancel
Update Server Settings:
Download Trusted and Optional Network policies
Update Client Settings:
Reset server configuration (IP address/Hostname, shared secret)
Expire Lease
Update Firebox's IPSec Certificate and CA's Certificate:
Issue/Reissue Firebox's IPSec Certificate and CA's Certificate

2 Change the settings as desired. The issue/reissue option forces a reissue of both the client and the root certificate. This is generally not necessary because a new certificate is downloaded every time the device is restarted.

Defining a Firebox as a DVCP Client (Dynamic Fireboxes Only)

If you are creating a tunnel to a Firebox with a dynamic IP address, you must define it as a DVCP client to enable VPN Manager to contact it.

From Policy Manager:

1 Select **Network** ⇒ **DVCP Client**.

2 Select the checkbox marked **Enable this Firebox as a DVCP Client**.

3 In the **Firebox Name** field, specify the name of the Firebox.

4 To log messages for the DVCP client, select the checkbox marked **Enable debug log messages for the DVCP Client**. (Selecting this option is not recommended unless you are currently troubleshooting.)

5 To add DVCP servers that the client can communicate with, click **Add**.

6 Enter the IP address. Enter the shared secret. Click **OK**.

7 Reboot the Firebox.
The Firebox contacts the DVCP server.

Adding Policy Templates (Required for Dynamic Devices)

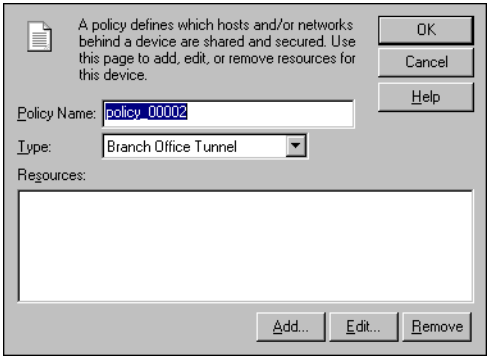
One of the benefits of a VPN is that you can define (and limit) the networks accessible through the tunnel: A VPN can be created between only two hosts or between multiple networks—or any combination in between. To define the networks available through a given VPN device, you create policy templates. By default, VPN Manager provides a network policy template that allows access to the network behind the VPN device to which the policy is applied. To create a policy template, on the **VPNs** tab:

1 Select the device for which you want to define a policy template.

2 Right-click and select **Insert Policy** or click the Insert Policy Template icon (shown at right).



The Device Policy dialog box for that device appears, as shown in the following figure.



3 Enter a policy name of your choosing.

4 Specify whether the tunnel is a branch office tunnel or a telecommuter tunnel (if the device is a SOHO 6).

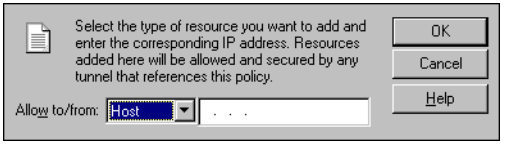
5 If you are defining a policy template for a Telecommuter tunnel, enter an unused IP address from the Firebox's trusted network. Enter the IP address of the machine behind the SOHO 6 that will use this tunnel.

6 Click **OK**.
The policy template is defined and is now available in the VPN Wizard when creating a VPN tunnel involving that device.

Adding resources to a policy template

From the **Device Policy** dialog box:

1 Click **Add**.
The Resource dialog box appears, as shown in the following figure.


Select the type of resource you want to add and enter the corresponding IP address. Resources added here will be allowed and secured by any tunnel that references this policy.
OK
Cancel
Help
Allow to/from:
Host

2 Select the type of resource you want and enter its IP address. Click **OK**.

Adding Security Templates

A security template specifies the encryption level and authentication type for a tunnel.

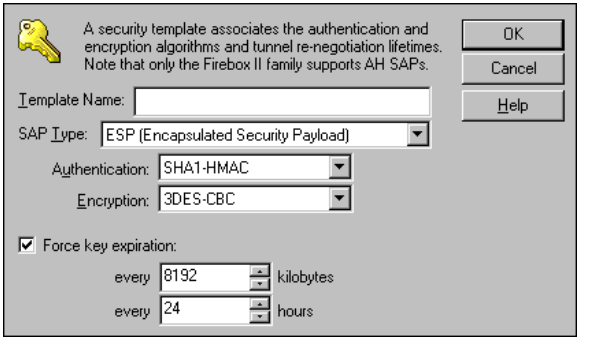
Default security templates are provided for available encryption levels. You can also create new templates. A variety of security templates makes it easy to match the appropriate level of encryption and type of authentication to the tunnel created with the Configuration wizard.

From the VPN Manager display:

1 Click the **VPN** tab.

2 Right-click anywhere in the window, and select **Insert Security Template** or click the Insert Security Template icon (shown at right).
The Security Template dialog box appears, as shown in the following figure.





3 Enter the template name, SAP (security authorization packet) type (either ESP or AH), authentication, and encryption.

4 If you want to force key expiration, select the corresponding checkbox, and then specify either kilobytes, hours, or both.
If you specify both, the key expires at whichever time arrives earliest.

The security template has been defined. It can now be selected in the VPN Wizard when creating a VPN tunnel involving that device.

5 Click **OK**.

Creating Tunnels Between Devices

You can define a tunnel either using the drag-and-drop method or the VPN Manager Configuration Wizard.

NOTE

You can add a factory default Firebox 500 to VPN Manager as a device, but you cannot create tunnels to it. To upgrade the Firebox 500 to support BOVPN, see "Enabling the BOVPN Upgrade" on page 317.

Drag-and-drop tunnel creation

Drag-and-drop tunnel creation has two restrictions:

- It cannot be used to create tunnels between two dynamic devices.
- Dynamic Fireboxes and SOHOs must have networks previously defined before using this method.

From VPN Manager:

1 Click the **Device** tab.

2 Click the device name of one of the tunnel endpoints to highlight it and drag it to the device name of the other tunnel endpoint.
This launches the VPN Manager Configuration Wizard, starting with the dialog box that shows (in two list boxes) the two endpoint devices you selected using drag-and-drop.

3 For each device (endpoint), select a policy template from the drop-down list.
The policy template determines the resources available through the tunnel. Resources can be a network or a host.
The listbox displays any policy templates you added to VPN Manager.

4 Click **Next**.
The wizard displays the Security Policy dialog box.

5 Select the security template appropriate for the level of security and type of authentication to be applied to this tunnel.
The listbox displays any templates you added to VPN Manager.

6 Click **Next**.
The wizard displays the DVCP configuration.

7 Select the checkbox marked **Restart devices now to download VPN configuration**. Click **Finish** to restart the devices and deploy the VPN tunnel.

NOTE

If you are configuring a large number of devices, you can delay restarting the devices until you have created all the tunnels. To restart any device, right-click it and select Restart. Or you can wait until a given device's lease expires, at which time VPN Manager uploads the new configuration automatically.

Menu-driven tunnel creation

This method is the only one you can use to create tunnels for dynamically addressed SOHO 6 devices.

From VPN Manager:

1 Click the **VPNs** tab.

2 Select **Edit** ⇒ **Create a New VPN** or click the Create New VPN icon (shown at right).

This launches the VPN Manager Wizard.

3 Click **Next**.
The wizard displays two listboxes that each list all the devices registered in VPN Manager.

4 Select a device from each listbox to be the endpoints of the tunnel you are creating.

5 Select the policy templates for each device's end of the tunnel.
The listbox displays any templates added to VPN Manager.

6 Click **Next**.
The wizard displays the Security Template dialog box.

7 Choose the appropriate security template for this VPN. Click **Next**.
The wizard displays the DVCP configuration.

8 Select the checkbox marked **Restart devices now to download VPN configuration**. Click **Finish** to restart the devices and deploy the VPN tunnel.

NOTE

If you are configuring a large number of devices, you can delay restarting the devices until you have created all the tunnels. To restart any device, right-click it and select Restart. Or wait until a given device's lease expires, at which time VPN Manager automatically uploads the new configuration.

Enabling a SOHO Single-Host Tunnel

Any SOHO (static or dynamic) can be configured for a tunnel that allows only one host behind the SOHO to connect to another endpoint (host or network). This tunnel is called a SOHO Telecommuter tunnel and is useful for situations where an employee sets up a home configuration such that his or her family's network is behind a SOHO, but only one computer—the telecommuter's—is allowed access to corporate resources available through the tunnel.

On the Firebox:

1 On the **VPNs** tab, under the **Devices** folder, select the device.

2 Right-click the device and select **Insert Policy**.
The Device Policy dialog box appears.

3 Enter the following:

Policy Name
Enter a friendly name of your choosing.

Type
Select **Telecommuter Tunnel** from the drop-down list.

Virtual IP Address Behind the Firebox
Enter a free IP address on the trusted network of the remote Firebox to which the SOHO is connecting.

Private IP Allowed to Use Tunnel
Enter the IP address of the trusted host behind the SOHO (the telecommuter's computer). Use the same address entered on the SOHO VPN configuration. Make sure that the telecommuter routes to 0.0.0.0/0 (default route through VPN).

On the SOHO:

1 Browse to the WatchGuard **SOHO Configuration** menu.
The default configuration IP address is 192.168.111.1.

2 Click **Managed VPN** from the menu on the left.

3 Select **Telecommuter** from the drop-down list.

4 Click **Enable Remote Gateway**.

5 Enter the following:

DVCP Server Address
Enter the IP address of the DVCP server (defined in VPN Manager) to which this device will be a client.

Client Name
Use the IP address or any identifying name or number. The same ID must be entered in VPN Manager when adding the device. If the SOHO has dynamic DNS, use the SOHO's dynamic DNS name.

Shared Secret
Enter a passphrase for use between the client and server. The same secret must be entered in VPN Manager when adding the device.

6 Click **Submit**.

Editing a Tunnel

All tunnels you have created are visible on the **VPNs** tab of VPN Manager. VPN Manager allows you to edit the tunnel name, security template, endpoints, and the policy used.

On the **VPNs** tab:

1 Expand the tree to show the device and its policy that you want to edit.

2 Highlight the tunnel that you want to edit.

3 Right-click and select **Properties**.
The Tunnel Properties dialog box appears.

4 Click **OK** to save the change.
When the tunnel is renegotiated, the changes are applied.

Removing Tunnels and Devices from VPN Manager

To remove a device from VPN Manager, you must first delete any tunnels for which that device is an endpoint.

Removing a tunnel

1 From VPN Manager, click the **VPNs** tab.

2 Expand the **Managed VPNs** folder to reveal the tunnel to be deleted.

3 Right-click the tunnel.

4 Select **Remove**. When asked to confirm, click **Yes**.

5 When prompted to issue a restart command to the devices affected by this removal, click **Yes**.

Removing a device

1 From VPN Manager, click either the **Devices** or **VPNs** tab.
Either the Devices tab (left figure below) or the VPNs tab (right figure below) appears.





Device tab (left) and VPN tab (right)

2 If you are using the **VPNs** tab, expand the **Devices** folder to reveal the device to be deleted.

3 Right-click the device.

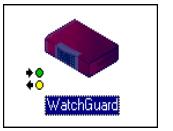
4 Select **Remove**. When asked to confirm, click **Yes**.

Allowing Remote Access to the DVCP Server

When running VPN Manager on a remote host, external from the Firebox designated as the DVCP server, you must allow incoming access.

From Policy Manager:

1 Double-click the WatchGuard icon, shown at right, in the Services Arena.



2 On the **Incoming** tab, select **Enabled and Allowed**.

3 Beneath the **From** field, click **Add**.
The Add Address dialog box appears.

4 Click **Add Other**.
The Add Member dialog box appears.

5 From the **Choose Type** drop-down list, click **Host IP Address**.

6 Enter the IP address of the VPN Manager station in the **Value** field. Click **OK**.

7 Under **To**, click **Add**.
The Add Address dialog box appears.

8 Click **Firebox**. Click **Add**. Click **OK**.

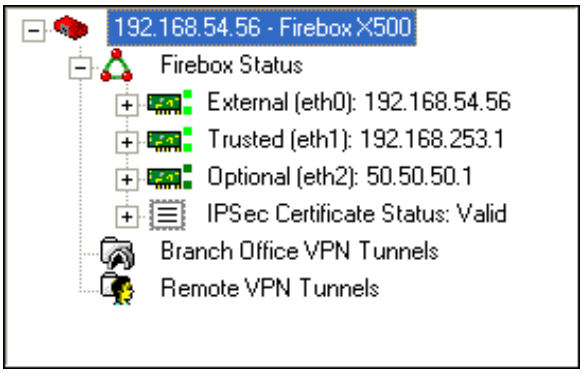
CHAPTER 24

Monitoring VPN Devices and Tunnels

To properly manage a VPN environment, you need real-time information on its components. Current status of all VPN devices and tunnels appears on Firebox System Manager and on the VPN Manager display. You can use this information to determine current device status, to diagnose problems, and to plan how various devices need to be configured or reconfigured.

Monitoring VPNs from System Manager

The **Front Panel** tab in System Manager shows the current status of the branch office, RUVPN, and MUVPN tunnels (both RUVPN and MUVPN tunnels are grouped under the Remote VPN Tunnels heading). The following figure shows the tunnel status information in System Manager.



Expanding and collapsing the display

To expand a branch of the display, click the plus sign (**+**) next to the entry, or double-click the name of the entry. To collapse a branch, click the minus sign (**–**) next to the entry. A lack of either a plus or minus sign indicates that there is no further information about the entry.

Red exclamation point

A red exclamation point appearing next to a device or tunnel indicates that something within its branch is not communicating properly. For example, a red exclamation point next to the Firebox entry indicates that the Firebox is not communicating with either the WatchGuard Security Event Processor or management station. A red exclamation point next to a tunnel listing indicates a tunnel is down.

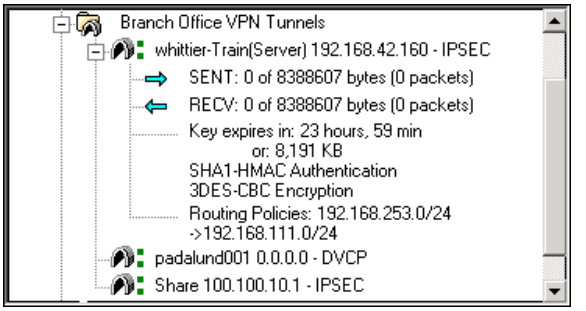
When you expand an entry with a red exclamation point, another exclamation point appears next to the specific device or tunnel with the problem. Use this feature to rapidly identify and locate problems in your VPN network.

Branch Office VPN tunnels

The first piece of VPN information displayed in System Manager is the status of branch office VPN tunnels. The figure below shows an expanded entry for a BOVPN tunnel. The information displayed, from top to bottom, is:

- The name assigned to the tunnel during its creation, along with the IP address of the destination IPSec device (such as

another Firebox, SOHO 6, or SOHO 6|tc), and the tunnel type (IPSec or DVCP). If the tunnel is DVCP, the IP address refers to the entire remote network address rather than that of the Firebox or equivalent IPSec device.


Branch Office VPN Tunnels
whittier-Train(Server) 192.168.42.160 - IPSEC
SENT: 0 of 8388607 bytes (0 packets)
RECV: 0 of 8388607 bytes (0 packets)
Key expires in: 23 hours, 59 min
or: 8,191 KB
SHA1-HMAC Authentication
3DES-CBC Encryption
Routing Policies: 192.168.253.0/24
->192.168.111.0/24
padalund001 0.0.0.0 - DVCP
Share 100.100.10.1 - IPSEC

- The amount of data sent and received on that tunnel in both bytes and packets.
- The time at which the key expires and the tunnel is renegotiated. Expiration time is expressed as a time deadline or in bytes passed. DVCP tunnels configured for both traffic and time deadline expiration thresholds display both; this type of tunnel expires when either event occurs first (time runs out or bytes are passed).
- Authentication and encryption levels set for that tunnel.
- Routing policies for the tunnel.

MUVPN and RUVPN tunnels

Following the branch office VPN tunnels is an entry for Mobile User VPN or RUVPN with PPTP tunnels.

If the tunnel is Mobile User VPN, the branch displays the same statistics as for the DVCP or IPSec Branch Office VPN described previously. The entry shows the tunnel name, followed by the destination IP address, followed by the tunnel type. Below are the packet statistics, followed by the key expiration, authentication, and encryption specifications.

If the tunnel is RUVPN with PPTP, the display shows only the quantity of sent and received packets. Byte count and total byte count are not applicable to PPTP tunnel types.

Monitoring VPNs through VPN Manager

You use the VPN Manager user interface to view real-time information on all managed devices simultaneously. This information is used to determine current device status, to diagnose problems, and to plan how various devices need to be configured or reconfigured.

The VPN Manager main window consists of four tabbed tree-view windows. The four tabs and descriptions of the information they contain are:

Device View
A status page for all devices in VPN Manager. The information that appears includes the log host, MAC address, and IP address for the interfaces for each device as well as the status of all VPN tunnels currently configured in VPN Manager.

VPN View
Displays status information on current VPN tunnels, their endpoints, and their security parameters.

Logging View
Displays the logging status for devices managed by VPN Manager.

Custom View
Provides a means for you to create a custom view of the devices managed by VPN Manager.

Opening the VPN Manager Display

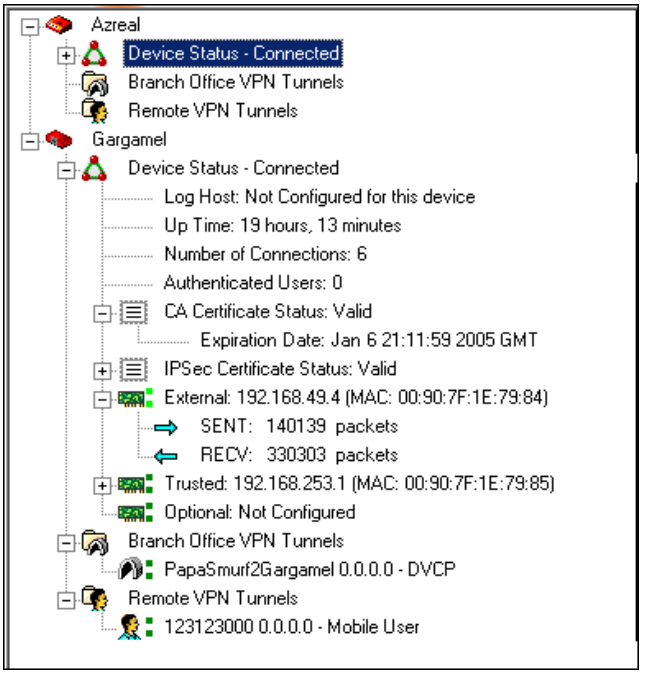
To open VPN Manager, from the Windows interface:

1 Select **Start** ⇒ **Programs** ⇒ **WatchGuard** ⇒ **VPN Manager**. You may be prompted for the configuration passphrase of the Firebox designated as your DVCP server.
VPN Manager connects to the DVCP server and displays the VPN and device configuration, distributed appropriately among the four tabs on the display.

Device Status

Click the **Devices** tab of the VPN Manager display to view the real-time status of all devices being managed by DVCP. An

example of the information shown on this tab appears in the following figure.



All devices appear in a tree-view structure. When the box next to an entry contains a plus sign (**+**), the tree is collapsed. To expand it, click the plus sign. The tree view expands at that entry to display the properties of that device.

To collapse the display, click the minus sign (**–**) next to a device. The expanded tree disappears, leaving a single-line entry for that device.

Connection status

The top level of the tree view for each device will show a red, yellow, or no exclamation point. The exclamation point (or lack of it) provides the device's status, even when the tree view is not expanded. The statuses indicated are as follows:

No exclamation point

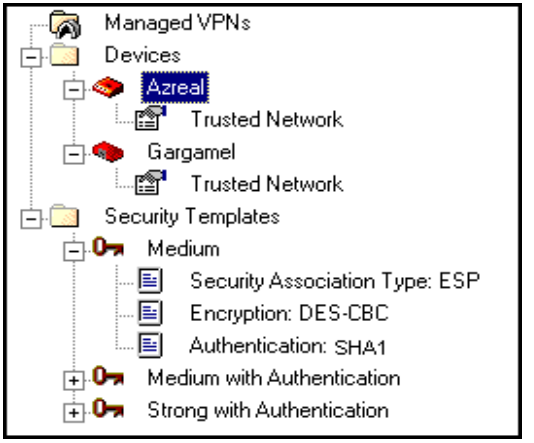
Normal operation. The device is connected to VPN Manager.

Yellow exclamation point
Questionable operation. VPN Manager is trying to contact the device. The exclamation point will either resolve or turn red.

Red exclamation point
Failed operation. The device is no longer connected to VPN Manager. Right-click the device, and select **Resume Connection**. If this fails to resolve the situation, examine the devices for other problems.

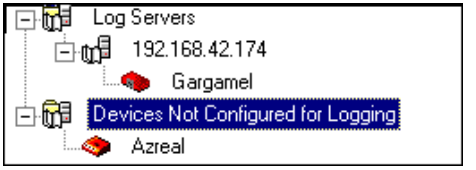
Tunnel status

Click the **VPNs** tab of the VPN Manager display to view the IPSec tunnels configured. This portion of the display, as shown in the following figure, includes information on devices and security templates, including security association type, encryption types, and authentication type.



Log server status

Click the **Logging** tab of the VPN Manager display to view log servers in the VPN environment. The list of servers in use is compiled from the configuration files of the devices under management. The display also lists devices for which logging is not configured. (Logging for devices is configured in Policy Manager, as described in Chapter 12, “Setting Up Logging and Notification.”)



Creating a custom view

The **Custom** tab of the VPN Manager display allows the creation of a customized workspace, optimized to your specific needs. Any of the resources in the Devices view can be listed on the **Custom** tab by tunnel location, level of encryption, device type used, and so on. The Firebox devices themselves (with all their corresponding settings and tunnel statistics), individual device statistics, individual tunnels, and individual remote users from any device can all be monitored. You can also create folders to group information in a way that is meaningful for your own environment.

For example, suppose your enterprise is very large, consisting of a hundred or more devices. You could use the custom view to group devices into manageable units according to variables such as region, business affiliation, operating units, and so on.

To add devices to the **Custom** tab:

1 In the **Device** tab of the VPN Manager display, right-click the device you want to add to the **Custom** tab.

2 Select the **Copy to Custom Tab** option.
The device appears on the Custom tab. You can select the device name and drag it to a new location in the window, or into a folder.

To add a folder on the **Custom** tab:

1 Right-click in the **Custom** tab window.

2 Select **Add New Folder**.

3 Double-click the name of the folder to select it. Enter a name for the folder.

CHAPTER 25

Managing the SOHO 6 with VPN Manager

VPN Manager allows you to manage and configure devices remotely. This is especially helpful when working with a SOHO 6 to set up a tunnel for an employee working offsite at a distant office or from his or her home.

Certain transactions in VPN Manager, such as managing a WatchGuard SOHO 6 remotely, require your Web browser to have certificates enabled. To maintain security in an open environment such as the Internet, the browser uses both a WatchGuard-proprietary encrypted socket protocol and Secure Sockets Layer (SSL)—the industry-standard method for protecting Internet communication.

Importing Certificates

When you define a Firebox as a DVCP server, a certificate file is created and stored in the directory where you installed the WatchGuard System Manager software. For example, a path of a certificate file might appear as follows:

```
c:\Program Files\WatchGuard\Certificates\[DVCP Server's IP Address]\SOHO-Admin.p12
```

This file must be imported by the browsers that will be used to contact and configure the SOHO 6 devices in your enterprise.

MS Internet Explorer 5.5 and 6.0

From the VPN Manager desktop:

1. Launch the browser and select **Tools** ⇒ **Internet Options**.
   The Internet Options window appears.
2. Click the **Content** tab. Click **Certificates**.
   The Certificates window appears.
3. Click the **Personal** tab. Click **Import**.
   The Certificate Import Wizard appears.
4. Click **Next**.
5. Browse to the file location, select it, and click **Open**.
6. Click **Next**.
7. Enter the configuration passphrase of the DVCP server and click **OK**.
8. Click **Next**.
9. Select the **Automatically select the certificate store based on the type of certificate** option, and then click **Next**.
10. Click **Finish**.
    A window appears indicating that the certificate has been successfully imported.

Troubleshooting tips

If any of the preceding steps fail, check the following:

- Verify that you have the strong encryption (128-bit) version of Internet Explorer.
- Verify that you have the correct password for the `.p12` (or `.pfx`) file. This must be the configuration passphrase of the Firebox that is acting as your DVCP server.
- Verify that the certificate file is not zero (0) length. If it is, delete the file, disconnect from VPN Manager, and run it again.
- Sometimes, at installation, Internet Explorer does not enable strong encryption. You can check this by looking in the registry. Look at

  ```
  HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Defaults\
  Provides\001
  ```

This should be set to Microsoft Enhanced Cryptographic Provider v1.0. If not, edit the line to fix it manually, and restart the browser.

Netscape Communicator 4.79

From the VPN Manager desktop:

1. Launch the browser and select **Communicator ⇒ Tools ⇒ Security Info**.
   The Security Info window appears.
2. From the navigation menu on the left, select **Certificates ⇒ Yours**.
3. Click **Import a Certificate**.
   The File to Import window appears.
4. Browse to the file location, select it, and click **Open**.
   The Password Entry Dialog box appears.
5. Enter the configuration passphrase of the DVCP server and click **OK**.
   A window appears indicating that the certificate has been successfully imported.
6. Click **OK** to return to the Certificates window.
   The imported certificate appears within the appropriate field.
7. Click **OK** to return to the browser.

Netscape 6

From the VPN Manager desktop:

1. Launch the browser and select **Tasks ⇒ Privacy and Security ⇒ Security Manager**.
   The Netscape Personal Security Manager window appears.
2. Click the **Certificates** tab.
3. From the navigation menu on the left, click **Mine**.
4. Click **Restore**.
   The File Name to Restore window appears.
5. Browse to the file location, select it, and click **Open**.
   The Password window appears.
6. Enter the configuration passphrase of the DVCP server and click **OK**.
   A window appears indicating that the certificate has been successfully restored.

7 Click **OK** to return to the Personal Security Manager window.
The imported certificate appears within the appropriate field.
8 Click **Close** to return to the browser.

Troubleshooting tips

If any of the preceding steps fail, check the following:

- Verify that you have the strong encryption (128-bit) version of Netscape.
- Verify that you have the correct password for the `.p12` (or `.pfx`) file. This must be the configuration passphrase of the Firebox that is your DVCP server.
- Verify that the certificate file is not zero (0) length. If it is, delete the file, disconnect from VPN Manager, and run it again.

Accessing the SOHO 6

Now that you have imported the proper certificate into your browser, you are ready to use VPN Manager to remotely access the device to monitor and manage the SOHO 6.

You cannot use the same browser to access the SOHO 6 as the one used to access the CA Manager. For more information on accessing the CA Manager, see "Managing the Certificate Authority" on page 278. You must close the CA Manager browser before attempting to access the SOHO 6 from VPN Manager.

From VPN Manager:

1 Select the SOHO 6 device you want to access and then click the SOHO Management icon on the toolbar (to the right of the Policy Manager icon).
The Client Authentication dialog box appears.
2 Select the certificate for this device and click **OK**.
3 Click **OK**.
The SOHO System Status page appears.

All SOHO 6 management functions that would normally be available locally through a Web browser are now available remotely and securely.

System Status

The System Status page is effectively the configuration home page of the SOHO 6. A variety of information is revealed to provide a comprehensive display of the SOHO 6 configuration:

- The firmware version
- A few of the SOHO 6 features and their status as Enabled or Disabled
- Upgrade options and their status
- Configuration information for both the trusted and external networks
- Firewall settings (Incoming and Outgoing services)
- A reboot button to restart the SOHO 6

Network

From the Navigation bar on the left, click **Network** to:

- Configure the SOHO 6 network settings for both the external and trusted networks
- Configure static routes in order to pass traffic to networks on separate segments
- View a variety of network statistics to assist in monitoring data traffic as well as troubleshooting potential problems

Administration

From the Navigation bar on the left, click **Administration** to:

- Enable System Security passphrases and allow Remote Management
- Enable VPN Manager access
- Update the SOHO 6 from a non-Windows operating system
- Upgrade the SOHO 6 features
- View the configuration file as text

System security and remote management

Here you enable system security, assign an administrator name to the device, and set the passphrases.

You can also enable the SOHO 6 for remote management. This allows you to connect to the unit remotely using the WatchGuard Remote Management VPN client. Set the virtual IP

address to be provided to your remote computer upon connection as well as the authentication and encryption algorithms used to secure the connection.

Firewall

From the Navigation bar on the left, click **Firewall** to:

- Configure the incoming and outgoing services.
- Define blocked sites
- Enable various firewall options, such as:
  - Do not respond to Ping requests received on external network
  - Do not allow FTP access to trusted network interface
  - Disable SOCKS proxy
  - Log all allowed outbound access
- Configure an unrestricted passthrough IP address for a single host

Logging

From the Navigation bar on the left, click **Logging** to:

- View the SOHO 6 Event Log—this displays various log entry messages
- Configure the SOHO 6 to send logs to a WSEP (WatchGuard Security Event Processor)
- Configure the SOHO 6 to send logs to a Syslog server
- Configure the System Time

WebBlocker

From the Navigation bar on the left, click **WebBlocker** to enable and configure this feature. WebBlocker filters your users' access to Web sites by category.

VPN

From the Navigation bar on the left, click **VPN** to:

- Configure VPN tunnels between the SOHO 6 and other IPSec-compliant devices
- Configure MUVPN clients to create Mobile User VPN tunnels to the SOHO 6
- View various statistics regarding existing tunnels

- Configure the ”Keep Alive” feature that sends a ping through a VPN tunnel so the tunnel won’t time out.

Removing Certificates

Certain situations might require you to update the certificates that VPN Manager uses. For example, if the configuration pass-phrase of the Firebox defined as the DVCP server is changed or if you are reinstalling the DVCP server, you will need to update the certificates. The certificates must be removed, and then new certificates must be generated and used.

MS Internet Explorer 5.5 and 6.0

From the VPN Manager desktop:

1 Launch the browser and select **Tools** ⇒ **Internet Options**.
The Internet Options window appears.

2 Click the **Content** tab. Click **Certificates**.
The Certificates window appears.

3 Select the certificate or certificates you want to remove.

4 Click **Remove**.
A warning window appears.

5 Click **Yes**.
The selected certificates are deleted from the browser.

6 Click **Close** and then click **OK** to return to the browser.

After you have removed the certificates from your browser, you must delete them from your computer.

From VPN Manager:

- Select **File** ⇒ **SOHO Management** ⇒ **Clean up on PC**.

Netscape Navigator 4.79

From the VPN Manager desktop:

1 Launch the browser and select **Communicator** ⇒ **Tools** ⇒ **Security Info**.
The Security Info window appears.

2 From the navigation menu on the left, select **Certificates** ⇒ **Yours**.

3 Select the certificate or certificates you want to remove.

4 Click **Delete**.
A warning window appears.
5 Click **OK**.
The selected certificates are deleted from the browser.
6 Click **OK** to return to the browser.

After you have removed the certificates from your browser, you must delete them from your computer.

From VPN Manager:

- Select **File ⇒ SOHO Management ⇒ Clean up on PC**.

Netscape 6

From the VPN Manager desktop:

1 Launch the browser and select **Tasks ⇒ Privacy and Security ⇒ Security Manager**.
The Netscape Personal Security Manager window appears.
2 Click the **Certificates** tab.
3 From the navigation menu on the left, select **Mine**.
4 Select the certificate or certificates you want to remove.
5 Click **Delete**.
A warning window appears.
6 Click **Delete**.
The selected certificates are deleted from your browser.
7 Click **Close** to return to the browser.

After you have removed the certificates from your browser, you must delete them from your computer. From VPN Manager:

- Select **File ⇒ SOHO Management ⇒ Clean up on PC**.

CHAPTER 26

Troubleshooting Firebox Connectivity

This chapter provides three ways of connecting to your Firebox should you lose connectivity. These procedures assume that you have already created a configuration file and will be restoring the Firebox with that file. If you have not yet created a configuration file, use the QuickSetup Wizard to create one, as described in Chapter 3, "Getting Started."

Loss of connection to the Firebox can occur because you lost or forgot your passphrases, you received a new Firebox as a replacement unit, or other reasons. But regardless of the reason you lost connectivity, you can use any of these methods to reconnect to your Firebox.

Although certain procedures vary slightly between Firebox X models and Firebox III models, the overall concepts are identical.

Method 1: Ethernet Dongle Method

This method involves using a single crossover cable.

1 Make sure the Firebox and the management station are disconnected from the network.

2 Connect one end of the crossover cable to the optional interface and the other end to the external interface

(labeled "2" and "0", respectively, on a Firebox X), creating a loop. Power-cycle the Firebox.

On a Firebox X, the LCD panel displays the following:
Firebox X<model number>
SysB - Loopback

On a Firebox III, the following light sequence appears:
Armed light: steady
Sys A light: flickering
(Do not be concerned with the lights on the security traffic display indicating traffic between interfaces.)

3 Disconnect the crossover cable from the optional and external interfaces. Now, connect one end to the trusted interface (labeled "1" on a Firebox X) and the other end to the management station. Do not turn off the Firebox.

4 Make sure the management station has a static IP address. If it doesn't, change the TCP/IP settings to a static IP address. The computer designated as the management station should be on the same network as the configuration file, preferably the trusted network, so you do not need to reassign an IP address to your computer after the configuration file has been uploaded.

The following is an example of a typical IP address scheme:
Management station: 192.168.0.5
Subnet mask: 255.255.255.0
Default gateway: 192.168.0.1
Trusted network: 192.168.0.1 (from the configuration file)

5 It is recommended that you double-check the IP address of the management station. To do this, open a DOS prompt and type `ipconfig /all`.

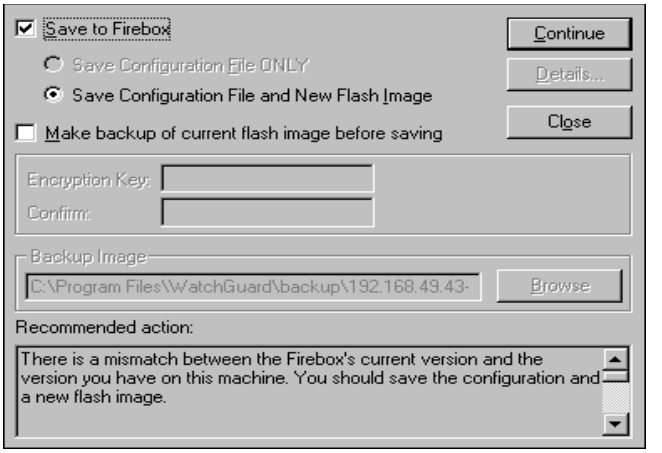
6 Use the Ping command to assign the Firebox a temporary IP address so your management station can communicate with the Firebox. At the DOS prompt, type `ping 192.168.0.1` (this is the default gateway of your computer). You will then see a request timeout. Ping again. You should get four replies.

7 Open Policy Manager from Firebox System Manager. Do not connect to the Firebox at this time.

8 In Policy Manager, select **File ⇒ Open ⇒ Configuration File**. Select the configuration file you want to load onto the Firebox and load it into Policy Manager.

9 In Policy Manager, select **File ⇒Save ⇒To Firebox**. You are then prompted for the IP address of the Firebox and the Firebox configuration passphrase. Use the address you used to ping the Firebox and `wg` for the passphrase.

10 When the **Firebox Flash Disk** dialog box appears, as shown in the following figure, select the button marked **Save Configuration File and New Flash Image**. Make sure the checkbox marked **Make Backup of current flash image before saving** is not selected.


Save to Firebox
Continue
Save Configuration File ONLY
Details...
Save Configuration File and New Flash Image
Close
Make backup of current flash image before saving
Encryption Key:
Confirm:
Backup Image
C:\Program Files\WatchGuard\backup\192.168.49.43-
Browse
Recommended action:
There is a mismatch between the Firebox's current version and the version you have on this machine. You should save the configuration and a new flash image.

After the configuration has been uploaded and the Firebox has been rebooted, the Firebox X LCD panel displays:

Firebox X<model number>
SysB - Loopback

The Firebox III light sequence should look like this:

Armed light: Steady
Sys A light: Steady

You should be able to ping the Firebox again with the same IP address you used earlier. At this point, you should be able to connect back to the Firebox through System Manager and reinstall the Firebox back into the network.

Method 2: The Flash Disk Management Utility

Like the first procedure, this method requires that you disconnect your management station and Firebox from the network.

1. Make sure the management station has a static IP address. If it doesn't, change the TCP/IP settings to a static IP address. The computer designated as the management station should be on the same network as the configuration file, preferably the Trusted network, so you do not need to reassign an IP address to your computer after the configuration file has been uploaded.
   The following is an example of a typical IP address scheme:
   Management station: 192.168.0.5
   Subnet mask: 255.255.255.0
   Default gateway: 192.168.0.1
   Trusted interface: 192.168.0.1 (from the configuration file)
2. Connect the blue serial cable to the Console port of the Firebox and the other end to the open COM port of the management station.
3. Connect the crossover cable from the Trusted interface on the Firebox (labeled "1" on a Firebox X) to the management station.
4. Access the Flash Disk Management utility: in System Manager, click the main menu button (shown at right). Select **Tools ⇒Advanced ⇒Flash Disk Managament**.



5. From the first screen in the Flash Disk Management tool, select **Boot from the System Area (Factory Default)**. Click **Continue**.
6. When prompted to enter an IP address, it is recommended that you use the address that is currently configured as the default gateway on your management station. Click **OK**.
7. Choose the COM port that is open on the management station. Click **OK**.
   This completes the Flash Disk Management utility.

8 Power-cycle the Firebox and wait until the operation has been completed.

On a Firebox X, the LCD panel displays the following:
Firebox X<model number>
SysB - Loopback

On a Firebox III, the light sequence should look like this:
Armed light: Steady
Sys B light: Steady (Some Fireboxes may flicker but most will be steady.)
(Do not be concerned with the lights on the security traffic display indicating traffic between interfaces.

9 Open a DOS prompt and ping the IP address that you used for the temporary IP.

Replies should follow, which means the Firebox is now ready for uploading a configuration.

10 In Policy Manager, select **File ⇒Open ⇒Configuration File**. Select the configuration file you want to load onto the Firebox and load it into Policy Manager.

11 In Policy Manager, select **File ⇒Save ⇒To Firebox**. You are then prompted for the IP address of the Firebox and the Firebox configuration passphrase. Use the address you used as the temporary IP address during the flash disk management process and `wg` as the passphrase.

12 When the **Firebox Flash Disk** dialog box appears, click the button marked **Save Configuration File and New Flash Image**.

After the configuration has been uploaded and the Firebox has been rebooted, the Firebox X LCD panel displays this:

Firebox X<model number>
SysA - Armed

On a Firebox III, the light sequence should look like this:

Armed light: Steady
Sys A light: Steady

You should be able to ping the Firebox again with the same IP address you used earlier. At this point, you should be able to connect back to the Firebox through System Manager and reinstall the Firebox into the network.

Method 3: Using the Reset Button

Before you start, assign the IP address of your management station to be on the 192.168.253.0 network. Do not use the 192.168.253.1 address, which is being held by the Firebox as a default. The subnet is 255.255.255.0.

It is recommended that you give your computer's default gateway an IP address of 192.168.253.1.

1 Disconnect the Firebox from the network.

Start with the Firebox turned off. Hold down the Reset button on the back of the Firebox (for Firebox III) or the Up arrow (for Firebox X) and turn on the Firebox power switch. On a Firebox X, you can release the Up arrow when the LCD display shows "Booting SysB."

On a Firebox III, do not let go of the Reset button until you see this light sequence:

External light on Triangle: Blinks
Trusted ⇒Optional traffic (Activity): Flashing lights
Sys B: Flickering
Armed: Steady

2 Connect a crossover cable to the management station and into the Firebox trusted interface (labeled "1" on the Firebox X).

3 Open a DOS prompt, and ping the Firebox with 192.168.253.1. You should get a reply.

4 In Policy Manager, select **File ⇒Open ⇒Configuration File**. Select the configuration file you want to load onto the Firebox and load it into Policy Manager.

5 In Policy Manager, select **File ⇒Save ⇒To Firebox**. When you are asked for the IP address of the Firebox, use 192.168.253.1 with `wg` as the passphrase.

6 When the **Firebox Flash Disk** dialog box appears, click the button marked **Save Configuration File and New Flash Image**.

7 After the file has been restored on the Firebox, you will have to reassign the IP address of your management station such that it is on the same network as the trusted interface from

configuration file that you just used. This will enable you to reconnect to the Firebox.

After the configuration has been uploaded and the Firebox has been rebooted, the Firebox X LCD panel displays this:

Firebox X<model number>
SysA - Armed

On a Firebox III, the light sequence should look like this:

Armed light: steady
Sys A light: steady

Index

Symbols

.cfg file. See configuration file
.ftr files 222
.idx files 204
.p12 file 273
.rep files 217
.wgl files 204
.wgx files 273
<$NOPAGE 67

Numerics

1-1 Mapping dialog box 104
1-to-1 NAT. See NAT, 1-to-1
3DES 251, 260

A

active connections on Firebox, viewing 91
ActiveX applets 143
Add Address dialog box 102, 118, 151, 288, 331
Add Exception dialog box 99, 105
Add External IP Address dialog box 103
Add External IP dialog box 102
Add Firebox Group dialog box 156
Add IP Address dialog box 188
Add Member dialog box 119, 152, 331
Add Port dialog box 114
Add Route dialog box 63, 64
Add Routing Policy dialog box 313, 315
Add Static NAT dialog box 102
address space probes, blocking 167
Advanced dialog box 54, 56
Advanced NAT Settings dialog box 99, 104
Aggressive Mode 307
AH
  configuring 310
  described 249, 309
aliases
  adding 151
  deleting 152
  described 149, 150
  dvcp_local_nets 150
  dvcp_nets 150

external 150
firebox 150
host 150
modifying 152
optional 150
trusted 150
Aliases dialog box 151
anonymous FTP 109
Any service
and RUVPN 286
precedence 122
ARP cache, flushing 78
ARP table, viewing 89
attacks, spoofing. See spoofing attacks.
attacks, types of 165
AUTH types for ESMTP 129
Authenticated Headers. See AH
authentication
CRYPTOCard server 160
defining groups for 155
DES, TripleDES 251
described 149, 152, 250
for VPNs, viewing 74, 335
from external interface 153
from optional interface 153
from outside Firebox 152
Java applet for 152
selecting method for 259
specifying server type 154
viewing types used 84
authentication servers
CRYPTOCard 161
described 250
network location for 154
RADIUS 158
SecurID on RADIUS server 162
types 153
types supported 288
viewing IP addresses of 84
Windows NT 157
Authentication Servers dialog box 155, 157, 158, 160, 162, 284
auto-block duration, changing 174

B

Bandwidth Meter tab 81
bandwidth usage, viewing 81
Basic DVCP Server Configuration dialog box 298, 301, 302
Berkeley Internet Name Domain (BIND) 144
blocked ports
auto-blocking sites that attempt to use 178
avoiding problems with legitimate users 177
default 175
described 174
logging activity 178
permanent 177
reasons for 175
setting logging and notification for 201
Blocked Ports dialog box 177, 178
Blocked Ports list 177
blocked services
NetBIOS 177
Novel IPX over IP 176
OpenWindows 176
rcp 176
rlogin 176
RPC portmapper 176
rsh 176
X Font server 175
X Window 175
blocked sites
and Firebox interfaces 172
and IDS applications 180
auto-block duration 174
auto-blocked 171
blocking with service settings 179
changing auto block duration 174
described 171
dynamic 179
exceptions to 173
in System Manager 84
logging and notification 174
permanent 171, 172

removing 174, 177
storing in external file 173
temporary 179
viewing list of 179
Blocked Sites dialog box 172, 174, 201
Blocked Sites Exceptions dialog box 174
Blocked Sites list
described 167, 179
exceptions to 173
viewing 90, 179
BOVPN
and certificate-based authentication 255
described 254
monitoring tunnels 334
BOVPN Upgrade
described 5, 31, 251, 298, 303
enabling 317
BOVPN with Basic DVCP
creating tunnel to SOHO 298
modifying tunnels 300
removing tunnels 301
requirements for 298
scenario 268
setting encryption type 299
setting logging options for 301
specifying authentication method 299
specifying encryption 299
specifying key expiration time 300
when to use 265
BOVPN with Manual IPSec
adding gateways 304
advantages of 256
allowing access to services 317
changing IPSec policy order 315
configuring a gateway 304
configuring a tunnel with manual security 308
configuring AH 310
configuring key negotiation type 305
configuring services for 316
configuring tunnels with dynamic key negotiation 311
creating routing policies 312
described 256, 303
editing, removing gateways 308
enabling Aggressive Mode 307
enabling Perfect Forward Secrecy 307
encryption levels 256, 303
Phase 1 settings 306
Phase 2 settings 308, 311
requirements for 304
selecting bypass rule 313
specifying authentication method 306, 307
specifying Diffie-Hellman group 307
specifying encryption 307
using certificates 306
using Encapsulated Security Protocol 310
when to use 265
BOVPN with VPN Manager
adding devices to 321
adding policy templates 324
adding security templates 325
allowing remote access to DVCP server 331
creating tunnels 326, 327
defining Firebox as DVCP client 323
described 256
editing tunnels 330
enabling SOHO single-host tunnel 328
removing devices and tunnels 330
scenario 268
when to use 266
branch office VPN. See BOVPN
bypass rules for tunnels 313

C

CA. See certificate authority
cables
connecting to Firebox 33
included with Firebox 22
cacert.pem 273
certificate authority
described 260, 271

designating as subordinate 279
designating Firebox as 275
enabling debug log messages for 276
Firebox as 120
Firebox as, scenarios 274
managing 278
restarting 280
scenarios 272
certificate revocation list (CRL)
described 272
publication period for 276
publishing 279
selecting endpoint for 276
certificates
and logging 277
described 250, 260, 272
destroying 280
generating new 278
importing to VPN Manager 341
listing current 279
publishing 280
reinstating 280
removing 347
revoking 280
searching for 279
setting lifetimes of 276
viewing CA fingerprint 73
viewing expiration date and time of 73
viewing status of 72
certificates, root. See root certificate
certification 19
CHAP authentication 158
classroom training 19
configuration file
and Policy Manager 43
basic 35
customizing 39
opening 43
opening from Firebox 44
opening from local drive 44
rebooting Firebox after saving 44
saving 44
saving to Firebox 45
saving to local drive 46
starting new 52
using existing 22
configuration modes
choosing 28, 35
setting using Policy Manager 52
Configure Gateways dialog box 305, 308
Configure Tunnels dialog box 308, 311
Connect to Firebox dialog box 69, 78
context-sensitive help 16
controld 208
controld.wgc 211
CRL. See certificate revocation list
CRYPTOCard server authentication 160, 161
custom program, as notification 122, 199

D

DCE 106
DCE-RPC, and NAT 106
debug logging, enabling for DVCP server 276
default gateways
entering 36
for Firebox interfaces 53
setting 54
viewing IP address of 73
default packet handling
and intrusion detection 179
blocking address space probes 167
blocking IP options attacks 168
blocking port space probes 167
blocking spoofing attacks 166
blocking SYN Flood attacks 168
described 166
logging and notification for 200
Default Packet Handling dialog box 167, 168, 169, 201
Define Exceptions dialog box 237
deny messages
copying 77

issuing ping or traceroute command for 77
SMTP proxy 130
DES 251, 260
Device Policy dialog box 324, 325
devices
adding to VPN Manager 321
dynamic 321
dynamic, and drag-and-drop 326
removing from VPN Manager 330
updating settings of 322
viewing connection status of 337
viewing status 336
DHCP 59
DHCP server
adding subnets 60
default lease time for 60
described 59
enabling 119
lease times 59
maximum lease time for 60
modifying subnets 61
not using Firebox as 59
removing subnets 61
setting up Firebox as 59
DHCP Server dialog box 59
DHCP Subnet Properties dialog box 60
DHCP support on external interface 30, 36, 54
dialog boxes
1-1 Mapping 104
Add Address 102, 118, 151, 288
Add Exception 99, 105
Add External IP 102
Add External IP Address 103
Add Firebox Group 156
Add Member 119, 152
Add Port 114
Add Routing Policy 313, 315
Advanced 54, 56
Advanced NAT Settings 99, 104
Aliases 151
Authentication Servers 155, 157, 158, 160, 162, 284
Basic DVCP Server Configuration 298, 301, 302
Blocked Ports 178
Blocked Sites 172, 174, 201
Blocked Sites Exceptions 174
Configure Gateways 305, 308
Configure Tunnels 308, 311
Connect to Firebox 69, 78
Default Packet Handling 167, 168, 169, 201
Define Exceptions 237
Device Policy 324
DNS-Proxy Properties 145
Firebox Authentication 154
Firebox Flash Disk 45, 47
Firebox Name 48
Host Alias 152
HTTP Properties 141
HTTP Proxy 237
Incoming SMTP Proxy 128
Incoming SMTP Proxy Properties 132
IPSec Branch Office License 318
IPSec Configuration 305, 308, 313, 315, 318
IPSec Logging 302
Licensed Features 6
Logging and Notification 120, 174, 200
Logging Setup 188, 189
NAT Setup 99, 104
Network Configuration 52, 57, 64
New Firebox Configuration 48, 52
New Server 277
New Service 114
NIC Configuration 64
Outgoing SMTP Proxy 136
PAD Rules for DNS Proxy 146
PAD Rules for FTP Proxy 139
PAD Rules for SMTP Proxy 134
Remote Gateway 305
Remote User Setup 288
Report Properties 218, 219
Resource 325
Security Policy 327
Security Template 325, 328

Select Gateway 308
service Properties 111, 113, 117, 179
Services 111, 114
Set Log Encryption Key 211
Setup Firebox User 156, 284
Setup Remote User 285
Setup Routes 63
SMTP Properties 133
SMTP Proxy Properties 128, 130
Time Filters 218
Tunnel Properties 330
Update Device 322
WebBlocker Utility 232
dial-up connection, for out-of-band management 243, 244
Diffie-Hellman
described 251
groups 251, 307
digital certificates. See certificates
DMZ (Demilitarized Zone) 25
DNS proxy
adding 145
and file descriptor limit 146
and NAT 146
and security policy 109
described 144
enabling protocol anomaly detection for 145
DNS resolution 304
DNS server addresses 58
DNS servers, configuring 283
DNS-Proxy Properties dialog box 145
drop-in configuration
benefits and drawbacks of 28
characteristics 28
described 27
setting IP addresses in 52
setting optional properties 56
DVCP
and certificates 257
and VPN Manager 256
basic 255
described 255, 297
DVCP Client Wizard 297, 299, 301
DVCP clients
defining Fireboxes as 323
described 297
SOHOs as 299
DVCP cluster 272
DVCP server
allowing remote access to 331
as CA 272
described 255, 297
enabling debug logging 276
friendly name for 277
setting logging options for 301
DVCP server, creating 120
dvcp_local_nets 99, 105, 150
dvcp_nets 99, 105, 150
dynamic IP support. See DHCP support, PPPoE support
dynamic NAT. See NAT, dynamic
dynamic security, configuring a tunnel with 311
Dynamic VPN Configuration Protocol. See DVCP
dynamically blocked sites 179

E

electronic page, as notification 121
email
as notification 121
blocking address patterns 132
blocking file-name patterns 131
denying attachments 131
protecting against relaying 132
screening with SMTP proxy 127
selecting headers to allow 132
sent after triggering event 196
Encapsulated Security Protocol. See ESP
encryption 32, 33
activating strong 282
and RUVPN with PPTP 282
described 249, 251
for VPNs, viewing 335
levels of 249, 251
encryption for VPNs, viewing 74
encryption key

entering 46
when saving configuration file 46
ESMTP
AUTH types 129
configuring 128
keywords supported 128
ESP
configuring 310
described 249, 309
eth3, eth4, eth5. See three-port upgrade
Ethernet dongle method for troubleshooting 349
event processor. See WatchGuard Security Event Processor or log host
event, described 183
extended authentication
defining groups for 288
described 250, 253, 254
external alias 150
external caching proxy servers, configuring 143
external interface
described 25
dynamic addressing on 54
external network 25, 43

F

failover 5
failover logging 186
FAQs 7, 13
fbidsmate utility
described 180
using 180, 181
filter window in LogViewer 205
filtered services. See services.
Filtered-HTTP 141
Firebox 500, and BOVPN Upgrade 5, 317
firebox alias 150
Firebox Authentication dialog box 154
Firebox Flash Disk dialog box 45, 47
Firebox Installation Services 18
Firebox interfaces
adding secondary networks to 29
and trust relationships 68
described 25
setting IP addresses of 52
viewing IP addresses of 72
Firebox kernal routing table, viewing 88
Firebox Name dialog box 48, 197
Firebox passphrases. See passphrases
Firebox System Manager applications, launching 80
Firebox System Manager. See System Manager
Firebox X Model Upgrade 4
Fireboxes
and IDS applications 180
as CAs 260
as certificate authority 120
cables included with 22
changing interface IP address 54
changing polling rate 79
choosing a configuration 28
configuration modes 25
configuring for logging 186
configuring for out-of-band 244
configuring for RUVPN with PPTP 281
connecting cables 33
connecting to 69, 78
connecting via out-of-band 241
defining as a DHCP server 59
defining as DVCP clients 323
defining as DVCP server 275
described 41
designating as CA 272, 275
designating as DVCP server 320
designating log hosts 187
entering encryption key for 46
friendly names in log files, reports 48, 197
gateways for interfaces 53
interfaces. See Firebox interfaces
location in network 42
making outbound connections behind 295
model 48

network cards in 83
obtaining IP addresses dynamically 31
opening configuration file 43
opening configuration file from 44
package contents 21
reasons for loss of connection 349
resetting pass phrase 47
saving configuration file to 45
setting clock to log host's 190
setting time zone for 48
specifying model of 48
timeout value 44
traffic sent through 72
troubleshooting connectivity 349
using out-of-band 241
viewing active connections on 91
viewing bandwidth usage 81
viewing everyone authenticated to 89
viewing log messages generated by 75
viewing memory usage of 85
viewing uptime and version 82
Flash Disk management tool 352
FTP
and optional network 43
and security policy 109
FTP proxy
and NAT 106
configuring 138
described 138
enabling protocol anomaly detection 139
hazards of 138
fully meshed topology 262

G

gateways
adding 304
configuring 304
described 304
gateways. See also default gateways
groups
assigning users to 156
for authentication 155
in Windows NT 158
ipsec_users 155
pptp_users 155
groups, authentication 284

H

H323, and NAT 106
hardware requirements 4
hidden services, viewing 120
High Availability 5, 22, 72
Historical Reports
applying a filter 223
creating report filter 222
deleting a filter 223
described 2, 80
editing a filter 223
editing existing reports 217
manually running a report 224
opening 80
starting 216
starting new reports 216
time spans for 218
time zone 48
Historical Reports. See also reports
Host Alias dialog box 152
host aliases 150, 151
host routes, configuring 64
hosts
viewing blocked 84
viewing in HostWatch 94
hosts, log. See log hosts
HostWatch
choosing colors for display 94
connecting to a Firebox 93
described 2, 80, 91
display 92
modifying view properties 94
opening 80
replaying a log file 93
setting display properties 94
starting 92

viewing authenticated users 94
viewing hosts 94
viewing ports 94
HTTP Properties dialog box 141
HTTP proxy
and NAT 106
restricting MIME types for 142
HTTP Proxy dialog box 237
HTTP services
adding 141
and security policy 109
and WebBlocker 233
described 140
Filtered-HTTP 141
HTTP 141
Proxied-HTTP 140
hub-and-spoke configuration 263

I

IKE
and Diffie-Hellman group 307
and Phase 1 settings 306
described 250
logging options for 301
phase 1,2 251
incoming services
see entries under services
Incoming SMTP Proxy dialog box 128
Incoming SMTP Proxy Properties dialog box 132
Incoming tab 108, 120, 126
installation
adding basic services after 62
QuickSetup Wizard 35
via serial cable 33
via TCP/IP 34
interfaces, monitoring 86
internal network 25
Internet
accessing through PPTP tunnel 294
Internet Explorer 4
Internet Key Exchange. See IKE
Internet Security Association and Key Management Protocol. See ISAKMP
intrusion detection and prevention 165—182
intrusion detection system (IDS)
and fbidsmate utility 180
described 179
IP addresses
adding to services 118
and drop-in configuration 27
and routed configuration 27
and static NAT 101
and VPN design 260
changing 54
default gateways 73
entering 37
entering for RUVPN with PPTP 288
in example network 23
netmask 73
of authentication servers 84
of Firebox interfaces 52
of log hosts 83
typing 78
WINS/DNS servers 58
IP alias 30
IP options attacks, blocking 168
IPSec
benefits of 249
changing policy order 315
described 248
logging options for 301
making outbound connections behind a Firebox 295
with VPN 255
IPSec Branch Office License dialog box 318
IPSec Configuration dialog box 305, 308, 313, 315, 318
IPSec Logging dialog box 302
IPSec tunnels, and DHCP/PPPoE 31
ipsec_users 155
ISAKMP
and Diffie-Hellman groups 307
and gateways 306
described 251, 311

J

Java applets
  and Zip files 143
  for authentication 152

K

Keep Alive feature 347
key pairs 272
known issues 13

L

launch interval, setting 199
license key certificates 22
license keys
  enabling,managing 6
Licensed Features dialog box 6
LiveSecurity Gold Program 18
LiveSecurity Service
  activating 11
  benefits of 9
  broadcasts 10
  described 3, 39
  Rapid Response Team 10
local drive, opening configuration file from 44
log encryption key, setting 193, 211
log files
  consolidating 210
  copying 210
  copying entries 206
  copying log entries 206
  default location of 203
  described 203
  displaying and hiding fields 206
  exporting records 206
  forcing rollover 210
  names of 204
  opening 204
  packet event fields 208
  replaying in HostWatch 93
  saving to a new location 211
  searching 205
  searching by field 205
  searing by keyphrase 205
  sending to another office 212
  setting Firebox names used in 48
  viewing with LogViewer 203
  working with 209
log hosts
  adding 187
  as Windows 2000 service 191
  as Windows NT service 191
  as Windows XP service 191
  changing priority 189
  designating for Firebox 187
  editing settings 189
  primary 186
  removing 189
  reordering 189
  running on Windows 2000 191
  running on Windows NT 191
  running on Windows XP 191
  scheduling reports 196
  secondary 186
  setting clocks 190
  setting rollover interval 195
  starting 193
  stopping 193
  synchronizing 190
  synchronizing NT 190
  viewing 193
  viewing IP addresses of 83
log messages
  copying deny messages 76
  generated by Firebox 75
  issuing ping or traceroute on deny messages 76
log rollover 194
log servers, viewing 338
logging
  architecture 186
  blocked port activity 178
  described 183
  developing policies for 184
  enabling Syslog 188

failover 186
for blocked ports 178
for blocked sites 174
for CA 276
for DVCP server 301
setting rollover interval 195
specifying for SMTP proxy 133
synchronizing NT log hosts 190
logging and notification
configuring Firebox for 186
customizing by blocking option 197
customizing by service 197
default packet handling 200
defining for services 120
described 183
designating log hosts 187
for blocked sites and ports 201
global preferences 194
setting for a service 200
Logging and Notification dialog box 120, 174, 178, 200
logging options, viewing 84
Logging Setup dialog box 187, 188, 189
LogViewer
consolidating logs 210
copying log data 205
described 2, 80
displaying and hiding fields 206
exporting log file data 205
filter window 205
opening 80
searching by field 205
searching by keyphrase 204, 205
searching for entries 205
setting preferences 204
starting 204
time zone 48
viewing files with 203
working with log files 209

M

MAC address of interfaces, viewing 73
mail servers
and NAT 103
protecting against relaying 132
main menu button 71, 78
Make Backup of Current Flash Image checkbox 45
management station
connecting with out-of-band 245
described 31, 42
enabling for out-of-band 242
setting up 31
man-in-the-middle attacks 170
manual IPSec tunnels, and DHCP/PPPoE 31
manual security, configuring tunnels with 308
masquerading, for SMTP proxy 136
Maximum Incomplete Connections setting 170
MD5-HMAC 260, 300
meshed topology 262
messages, deny. See deny messages
MIME types
creating new 131, 142
described 129
restricting for HTTP proxy 142
minimum requirements 3
Mobile User VPN. See MUVPN
modems, installing for out-of-band management 242, 243
monitoring
active connections on Firebox 91
ARP table 89
Firebox activity 82
load average 85
network interfaces 86
processes 85
routes 88
MSDUN, and RUVPN 290
MUVPN
and certificates, scenarios 273
and IP addressing 261
and WINS/DNS server addresses 58
authentication for 252
described 5, 252
encryption levels for 252

monitoring tunnels 74, 335
scenario 269, 273
types of licenses for 252
when to use 266
with extended authentication 253, 270

N

name resolution, fixing slow 146
NAT
1-to-1
and dynamic NAT exceptions 100
and PPPoE support 31
described 96, 103
using 103
and DNS proxy 146
and mail servers 103
and tunnel switching 265
and VPNs 261
described 95
dynamic
described 95, 96
service-based dynamic
configuring exceptions 100
described 96
disabling 101
enabling 100, 101
using 100
simple dynamic
adding entries 98
defining exceptions 99
described 96
enabling 97
reordering entries 99
using 97
static
adding external IP addresses 101
configuring a service for 95, 101
described 95
setting for a service 102
typically used for 95
types of 95
types supported by proxies 105
NAT Setup dialog box 97, 99, 104
NetBIOS services 177
netmask, viewing address of 73
Netscape Communicator 4
network address translation. See NAT
network addresses, unconnected 172
network cards in Firebox 83
Network Configuration dialog box 52, 54, 57, 64
network configurations
choosing 28
diagram 26
drop-in 27
routed 26
Network Connection wizard 293
Network File System 176
network interfaces, monitoring 86
network routes. See routes
network topology
described 262
fully meshed 262
hub-and-spoke 263
partially meshed 263
network traffic. See traffic
networks
external 25
internal 25
viewing blocked 84
networks, secondary. See secondary networks
New Firebox Configuration dialog box 48, 52
New Server dialog box 277
New Service dialog box 114
NIC Configuration dialog box 64
notation, slash 37
notification
blocked port activity 178
bringing up popup window as 121
described 183
developing policies for 184, 185
example policy 185
for blocked ports 178
for blocked sites 174
running custom program as 122
sending email as 121
setting launch interval 199
setting repeat count 199
settings for 196

triggering electronic page as 121
Novel IPX over IP 176
NXT attacks 144

O

Online Help 13, 15
online support services
accessing 13
described 12
online training 13
OOB. See out-of band management
OpenWindows 176
optional alias 150
optional interface 25
optional network
and FTP 43
described 43
Web server 43
optional products
3-port upgrade 4
BOVPN upgrade 5
described 4
Firebox X model upgrade 4
High Availability 5
Mobile User VPN 5
purchasing 6
SpamScreen 5
VPN Manager 4
outgoing services
see entries under services
Outgoing SMTP Proxy dialog box 136
Outgoing tab 108
out-of-band management
and PPP connection 242
configuring dial-up connection for 243, 244
configuring Firebox for 244
configuring PPP 245
connecting Firebox using 241
described 241
enabling management station for 242
establishing connection 245
installing modem 242, 243
preparing NT Management Station for 242
preparing Windows 2000 Management Station for 242
preparing Windows XP Management Station for 243
timeout disconnects 245

P

packet filters, described 107
packet handling, default. See default packet handling
packet-handling services. See services
packets
viewing number allowed, denied, rejected 83
viewing number sent and received 73
PAD Rules for DNS Proxy dialog box 146
PAD Rules for FTP Proxy dialog box 139
PAD Rules for SMTP Proxy dialog box 134
PAD. See protocol anomaly detection
pager, as notification 121, 196
PAP authentication 158
partially meshed networks 263
passphrases
configuration 36
described 36
resetting for Firebox 47
status 36
tips for creating 47
password authentication 250
passwords
and security of VPN endpoints 260
described 250
PEM format 280
Perfect Forward Secrecy 307
permanently blocked sites 172
Phase 1
described 251
settings 306
Phase 2

described 251
settings 308, 311
ping command for source of deny messages 77
PKCS12 format 280
PKI 271
Policy Manager
as view of configuration file 43
described 2, 43, 80
opening 80
opening a configuration file 43
Services Arena 80
services displayed in 110
using to create configuration file 51
policy templates
adding 324
adding resources to 325
polling rate, changing 79
POP, and security policy 109
popup window, as notification 121, 199
port space probes
and default packet handling 179
blocking 167
ports
0 176
1 176
1000-1999 177
111 176
137 through 139 177
2000 176
213 176
513 176
514 176
additional. See three-port upgrade
speed and duplex settings 64
used for new services 115
viewing in HostWatch 94
ports, blocked. See blocked ports.
PPP connection, and out-of-band management 242, 245
PPP user name and password 30, 53
PPPoE support on external interface 30, 36, 54
PPPoE, static 56
PPTP 249
PPTP. See also RUVPN with PPTP
pptp_users 155, 284
private key, public key 272
private LAN 25
processes, viewing 85
processor load indicator 72
program, as notification 122
protocol anomaly detection
described 133
enabling for DNS proxy 145
enabling for FTP 139
enabling for SMTP 126
setting rules for 134
Proxied-HTTP 140, 233
proxies
and BOVPN tunnels 315
described 107
types of NAT supported 105
proxy ARP 28
proxy servers, setting up 143
Proxy service 233
proxy services
described 125
DNS 144
FTP 138
HTTP 140
SMTP 127
public key cryptography 272
Public Key Intrastructure (PKI) 271
public servers, configuring 36

Q

QuickSetup Wizard
described 35
launching 35
rerunning 35
running from System Manager 78
steps 35

R

RADIUS server authentication 158
Rapid Response Team 9, 10
rcp service 176
RealNetworks, and NAT 106
red exclamation point
  in System Manager display 334
  in VPN Manager display 338
  in VPN Monitor 75
Remote Gateway dialog box 305
Remote User Setup dialog box 288
Remote User VPN. See RUVPN with PPTP
repeat count, setting 199
Report Properties dialog box 218, 219
reports
  applying a filter 223
  authentication details 225
  authentication resolution on IP addresses 218
  consolidated sections 228
  consolidating sections 219, 224
  creating filters 222
  customizing 215
  deleting 217
  deleting a filter 223
  denied incoming/outgoing packet detail 227
  denied packet summary 227
  denied service detail 227
  detail sections 219
  DNS resolution on IP addresses 219
  editing 217, 218
  editing filters 223
  exporting to HTML 220
  exporting to text file 221
  Firebox statistics 225
  FTP detail 227
  host summary 225, 226
  HTTP detail 226
  HTTP summary 226, 229
  key issues 215
  location of 220
  NetIQ format 221
  network statistics 228
  proxy summary 226
  reasons for generating 215
  running manually 224
  scheduling 224
  sections in 218, 225
  service summary 225
  session summary 225, 226
  setting Firebox names used in 48, 220
  SMTP summary 226
  specifying sections for 218
  starting new 216
  summary sections 219
  time spans for 218
  time summary 226, 228
  using filters 222
  viewing list of 218
  WebBlocker detail 227
requirements
  hardware 4
  software 3
Resource dialog box 325
rlogin service 176
root certificate
  described 272
  publishing 279
  reissuing 280
  setting lifetime for 276
routed configuration
  benefits and drawbacks of 27
  characteristics of 27
  described 26
  setting IP addresses in 54
routes
  configuring 63
  described 62
  host 64
  monitoring 88
  network 63
routing policies
  changing order of 315
  configuring multiple 316
  creating 312
  described 256, 312

proxies over VPN tunnels 315
RPC portmapper 176
rsh service 176
RTSP, and NAT 106
RUVPN with PPTP
accessing the Internet with 294
activating 287
adding a domain name for NT 291
and authentication groups 284
and MSDUN 290
and the Any service 286
and WINS/DNS server addresses 58
configuration checklist 281
configuring debugging options 289
configuring services to allow 285
configuring shared servers for 283
described 253, 281
encryption levels 282
entering IP addresses for 288
IP addressing 261, 281
making outbound connections behind a Firebox 295
monitoring tunnels 74, 335
preparing client computers for 289
preparing Windows 2000 remote host 293
preparing Windows NT remote host 290
preparing Windows XP remote host 293
running 294
starting 294
when to use 266
with extended authentication 254

S

Save dialog box 46
Save Main Window dialog box 206
Scheduled Tasks, installing 240
secondary networks
adding 30, 36, 57
described 29
SecurID authentication 162
security applications 3
Security Parameter Index (SPI) 310
security policy
and DNS 109
and FTP 109, 138
and HTTP 109
and POP 109
and services 108
and SMTP 109
and telnet 109
customizing 39
described 39
guidelines for services 109
opening configuration file 43
Security Policy dialog box 327
Security Template dialog box 325, 328
security templates, adding 325
security traffic display
described 69
selecting center interface 71
switch between 3 port and 6 port 70
viewing Firebox status using 70
Select Gateway dialog box 308
Select MIME Type dialog box 130
service Properties dialog box 111, 113, 117, 179
service properties, using to block sites 179
service-based dynamic NAT. See NAT, service-based dynamic
services
adding 111
adding addresses 118
adding several of same type 113
allowing VPN access to 317
and your security policy 39, 108
basic 62
blocked. See blocked services.
commonly added 39
configurable parameters for 111
configuring for BOVPN with Manual IPSec 316
configuring for incoming static NAT 95
configuring for Static NAT 101

configuring to allow RUVPN traffic 285
creating new 114
custom 110
customizing logging and notification 120
customizing logging for 197
defining properties of 117
deleting 116
described 107
disabled 117
displayed in Policy Manager 110
enabled and allowed 118
enabled and denied 117
guidelines for incoming 109
guidelines for outgoing 109
hidden 120
HTTP 140
icons for 110
incoming and outgoing, defined 108
multiple 114
Novel IPX over IP 176
OpenWindows 176
overriding NAT setting 101
precedence 122
proxied-HTTP 233
Proxy 233
rcp 176
rlogin 176
RPC portmapper 176
rsh 176
setting logging and notification for 200
setting static NAT for 102
viewing number of connections by 82
wg_ 119
X Font service 175
X Window 175
Services Arena
described 80, 110
displaying detailed view 111
Services dialog box 111, 114
Set Log Encryption Key dialog box 211
Setup Firebox User dialog box 156, 284
Setup Remote User dialog box 285
Setup Routes dialog box 63, 64
SHA1-HMAC 300
SHA-HMAC 260
shared secrets 158, 250, 259
sites, blocked. See blocked sites.
slash notation 37
SMTP Properties dialog box 133
SMTP proxy
adding address patterns 132
adding content types 130
adding masquerading options 136
allowing headers 132
and MIME types 130
and NAT 106
and security policy 109
blocking file-name patterns 131
blocking MIME types 129
configuring 127
configuring outgoing 136
denying attachments 131
described 127
email relaying 132
enabling protocol anomaly detection 126
keywords supported 127
selecting headers to allow 132
specifying logging for 133
SMTP Proxy Properties dialog box 128, 130
SMTP, extended. See ESMTP
software requirements 3
SOHOs
as DVCP clients 298
creating tunnels for dynamic 327
creating tunnels to 298
remote management of 345
remotely accessing 344
single-host tunnels 328
SpamScreen 5, 22
split tunneling
with PPTP, enabling 294
spoofing attacks
and System Manager 84
blocking 167

described 166
static PPPoE 56
Steel Belted RADIUS 162
subnets
adding to DHCP server 60
modifying 61
removing 61
SYN flood attacks
blocking 168
changing settings 169
described 168
preventing false alarms 169
SYN Validation Timeout setting 170
Syslog color 76
Syslog logging
enabling 188
facilities 188
System Manager
ARP table 89
authentication host information 84
authentication list 89
basic Firebox status 71
Blocked Sites list 90
blocked sites list 84
changing polling rate 79
components of 333
described 2, 67
Firebox uptime 82
front panel 72
interfaces 86
load average 85
log and notification hosts 83
logging options 84
memory 85
monitoring tunnels in 73
monitoring VPNs from 333
network configuration 83
packet counts 83
processes 85
routes 88
running QuickSetup Wizard from 78
ServiceWatch tab 82
spoofing information 84
starting 68
Status Report tab 82
version information 82
viewing bandwidth usage 81
System Manager main menu button 280
system requirements 3

T

TCP/IP, cabling for 34
TCPmux service 176
Technical Support
assisted support 17
described 9
Firebox Installation Services 18
frequently asked questions 9
LiveSecurity Gold Program 18
LiveSecurity Program 17
users forum 13, 14
VPN Installation Services 18, 267
telnet, and security policy 109
third-party authentication server. See authentication or name of third-party server
three-port upgrade
and aliases 150
and network traffic 68
and security traffic display 69
and Status Report 86
described 4
ports provided with 26
Time Filters dialog box 218
time zone for Firebox, setting 48
timeout duration for Firebox 44
traceroute command for source of deny messages 77
traffic
incoming and outgoing, defined 67
monitoring 75
viewing using security traffic display 70
Traffic Monitor
copying deny messages in 77
described 75
issuing ping and traceroute command in 77

limiting messages 76
traffic volume indicator 72
training
and certification 19
classroom 19
online 13
TripleDES 251, 260
troubleshooting Firebox connectivity 349
trust relationships among Firebox interfaces 68
trusted alias 150
trusted interface 25
trusted network 42
TSIG attacks 144
Tunnel Properties dialog box 330
tunnel switching 265
tunneling protocols 248
tunnels
and gateways 304
and proxies 315
bypass rules for 313
configuring with dynamic security 311
configuring with manual security 308
created to dropped-in devices 314
creating to SOHOs 298
creating with Basic DVCP 298
creating with VPN Manager 319, 326
described 248
drag-and-drop creation 326
editing 330
menu-driven creation 327
Mobile User VPN 74
modifying Basic DVCP 300
monitoring 73, 334
multiple policies for 316
removing from VPN Manager 330
RUVPN with PPTP 74
SOHO single-host 328
viewing 338
viewing status of 72

U

unconnected network addresses 172
Update Device dialog box 322
Use Incoming Settings for Outgoing checkbox 309
user authentication. See authentication
users, viewing in HostWatch 94

V

virus alerts 11
VPN Installation Services 18, 267
VPN Manager
adding devices 321
and authentication via certificates 257
and DVCP 256
and wg_dvcp service 120
certificates in 341
creating custom view 339
described 4, 256, 319
launching 320
opening UI 336
physical description 336
removing certificates 347
UI 336
viewing device status 336
viewing log servers 338
viewing tunnels 338
VPNs
access control for 261
allowing incoming services from 109
and 1-to-1 NAT 103
and IP addressing 260
and IPSec 255
and NAT 261
authentication methods for 259
described 248
design considerations 259, 260, 262, 263, 267
in routed configurations 27
monitoring 333

monitoring from System Manager 333
monitoring with VPN Manager 336
network topology 262
scenarios 267
WatchGuard solutions 265

W

WatchGuard Certified Training Partners (WCTPs) 19
WatchGuard installation directory, and log files 211
WatchGuard security applications 3
WatchGuard Security Event Processor
accessing user interface 209
and certificates 277
and log files 203
and notification 183
and reports 215
described 42, 81
failover logging 186
installing 190
opening user interface 81
running reports 224
starting 193
stopping 193
user interface 193
WatchGuard service 233
WatchGuard System Manager
additional information on 79
components of 2
described 1
documentation 17
hardware requirements 4
introduction 2
Online Help 15
options 4
package contents 22
requirements 3
software requirements 3
Web browser requirements 4
WatchGuard users forum 14
WatchGuard users group 14
Web browser, requirements for WatchGuard System Manager 4
Web server, and optional network 43
Web sites, filtering 231
WebBlocker
activating 234
automatically downloading database 239
configuring 233
configuring message for 235
creating exceptions for 236
described 231
manually downloading database 240
prerequisites 231
required services 233
scheduling hours 235
setting privileges 236
time zone 48
WebBlocker server
and setup program 32
installing 231—232
installing multiple 238
managing 238
viewing status of 233
WebBlocker Server Bypass 234
WebBlocker utility 232
WebBlocker Utility dialog box 232
wg_ services
described 119
viewing 120
wg_authentication 119
wg_ca 120
wg_dhcp_server 119
wg_dvcp 120
wg_pptp 120
wg_sohomgt 120
wg_pptp service icon 287
WGReports.exe 216
What's This? help 16
Windows 2000
and WatchGuard System Manager requirements 3
preparing for RUVPN with PPTP 293
preparing Management Station for out-of-band management 242

running log host on 191
Windows NT
adding a domain name 291
and WatchGuard System Manager requirements 3
installing a VPN adapter on 292
local and global groups 158
preparing for RUVPN with PPTP 290
preparing Management Station for out-of-band management 242
running log host on 191
Windows NT Server authentication 157
Windows XP
and WatchGuard System Manager requirements 3
preparing for RUVPN with PPTP 293
preparing Management Station for out-of-band management 243
running log host on 191
WINS server addresses 58
WINS servers, configuring 283
wizard.cfg 35
WSEP. See WatchGuard Security Event Processor

X

X Font server 175
X Window 175
XAUTH. See extended authentication

Y

yellow exclamation point, in VPN Manager display 338

Z

Zip files 143